



Hi ,

Does it suddenly seem like everyone’s selling something sovereign? You’re not imagining it.

Canadian companies have discovered that simply invoking or gesturing at *sovereignty* sells. The Globe and Mail [noted](#) the word is suffering from the phenomenon of “semantic satiation.” If the concept was vague before, it now risks collapsing under the weight of its own overuse — stretched thin instead of elevated as a guiding principle.

Examples abound. Telus has a “[Sovereign AI Factory](#)” and Bell is [investing in sovereign AI capacity](#).

We noticed a recent episode of a popular Canadian politics podcast included multiple ads on the theme. An Interac ad claimed the company is making sure “the next generation of digital money runs on Canadian infrastructure,” while a Telus ad about its Canadian AI development noted the sovereignty risks inherent in relying on U.S. data centres. (It means Canadian data is subject to U.S. laws — an issue [SHIELD has also raised](#).)

“Sovereign cloud.” “Sovereign data.” “Critical minerals sovereignty.” “Canadian-made” AI models. The word taps into a national anxiety about control and independence. But what’s actually sovereign about these products and services? Often, not much. Or, not quite enough.

“Sovereignty-washing” is the new [greenwashing](#): an attempt to launder global dependencies through patriotic language. It’s designed to soothe, not to clarify. And it’s becoming harder to distinguish what genuinely serves the national interest from what merely claims to.

While domestic firms make their priorities known, a wave of “Canadian sovereign cloud” offerings is being deployed by foreign firms. Global hyperscalers like [Microsoft](#), [Google](#) and [AWS](#) now promote services hosted on Canadian soil, implying safety from foreign laws. But data *residency* is not the same thing as data *sovereignty*: residency refers to where the data sits geographically, and sovereignty is about who controls it. If the parent company is headquartered abroad, those servers remain subject to extraterritorial legislation like the U.S. [CLOUD Act](#) and the earlier [Foreign Intelligence Surveillance Act \(FISA\)](#). That means simple data localization doesn’t offer the liberation and protections Canadians deserve. Even if it did, we couldn’t demand it because [Chapter 19 of CUSMA](#) limits our ability to require American companies localize their data in Canada as a condition of doing business here.

Shared Services Canada is [on the hunt](#) for information about sovereign cloud capabilities. Its recent procurement notice provides an idea of what a domestic sovereign cloud should actually look like, and it is *not* what the hyperscalers are offering. The government agency’s minimum requirements for a sovereign cloud are that data (1) be processed, transmitted and stored exclusively in Canada, and (2) never subject to legislation that permits foreign governments to obtain access to that data without Canada’s consent.

The same sovereignty halo is being invoked in the artificial intelligence sphere. In recent weeks, Microsoft Canada’s CEO has taken to the business pages to [stress](#) the company’s commitment to continue investing in Canada even as the country looks to bolster domestic AI development. Meanwhile, [CBC News reported](#) OpenAI is seeking to partner with Ottawa on a data centre deal using a brash domestic sovereignty pitch that flatters Canada’s current AI capabilities, while seemingly aiming to get its own tech embedded here.

The implicit question — does trading away sovereignty continue to be the price of partnership? — hangs in the air. (The federal government’s decision to fund Cohere’s [partnership with U.S.-based CoreWeave](#) provides one answer.) Canada’s eagerness to attract global AI investment risks entrenching dependency on the very firms whose power Ottawa hopes to balance.

In an effort to introduce consistency, the Digital Governance Council has developed a Draft National Standard for Digital Sovereignty, and their Standards Committee is now reviewing the feedback that was obtained during a public review period. Their standard introduces a clear framework to help organizations assess and protect their capacity to control their own digital infrastructure, data, and technologies. It also proposes a foundational set of definitions for *digital sovereignty*—a timely contribution to Canada’s evolving digital policy landscape.

The uncertain branding of product-based sovereignty is a reminder of the blurry boundaries around what counts as “Canadian,” a live issue in this era of maple-washing and sovereignty-washing.

If you listen to the Green Party of Canada, even the federal government has mud on its face. The Greens have [pointed out](#) that elements of the federal government’s roster of key “nation-building” projects raise sovereignty concerns and will ultimately bolster foreign firms.

“Canadian” can be a legal reality or a marketing strategy — and we should be clear about which one is being sold to us.

The good news is that there’s already a legal framework that can be used to test basic sovereignty claims.

The Competition Act [prohibits](#) false or misleading representations. If a firm suggests its “sovereign” product offers immunity from foreign control when it doesn’t, that could count as deceptive advertising. The Competition Bureau has gone after broad marketing claims [like Rogers’ “unlimited data,”](#) signalling that “sovereign” slogans could be fair game too.

“Sovereignty” has become a marketing strategy; a compelling word companies use to sell control they can’t actually guarantee. But real sovereignty isn’t a slogan or a server location. It’s about who governs a system, who profits from it, and who gets to decide the rules.

If a product or platform promises “sovereign” protection while still being subject to foreign law or ownership, that’s not nation-building, it’s nation-branding. Canada already governs “Made in Canada” claims and “unlimited data” promises through existing regulations. Maybe it’s time to start truth-testing “sovereign” ones too.

The Fall Budget is a chance to move past the maple-leaf marketing and start building the real thing: a Canada that actually governs, not just gestures at, its own systems.

Have you noticed “sovereign” popping up as a way to sell something? We’re collecting examples, just reply to this email.

Until next time,
Vass Bednar

In the Sovereignty Conversation This Week

SHIELD took part in the [Canadian Chapter of the International Institute of Communications’ annual conference](#) to participate on a panel on *International Trade, CUSMA, and Canadian Sovereignty*—a timely discussion about how cultural and digital sovereignty fit into Canada’s trade architecture. The exchange highlighted that defending and building sovereignty today means governing not only goods and borders, but also code and culture. You can catch up on the sessions [here](#).

SHIELD was also in Ottawa for a Parliamentary Committee appearance, appearing before the [Trade Committee](#). Vass Bednar, Managing Director of the Canadian SHIELD Institute, argued that Canada’s next trade strategy must restore its epistemic sovereignty — the ability to audit and govern the digital systems shaping its economy. She urged MPs to use the upcoming CUSMA review to reclaim policy space over data, algorithms, and cloud infrastructure, warning that current trade rules limit Canada’s “freedom of thought.” Bednar also called for a modernized SAGIT system and National Economic Council to rebuild Canada’s trade intelligence for the digital era.

SHIELD was also in Montreal for [The Attention Forum](#), where we moderated a panel on reigning in tech monopolies with former Chair of the UK Competition and Markets Authority (CMA) Marcus Bokkerink and Y-Combinator’s Luther Lowe. The conversation focussed on future opportunities to support better competition, like interoperability and ending self-preferencing.

SHIELD In the News

A new [Tech Policy Press piece](#) from Policy Research Associate Emily Osborne asks what a “sovereign cloud” really means — and who it actually serves. While U.S. tech giants now market “sovereign” options, the article notes these services still fall under U.S. law, leaving Canadian data exposed. True digital sovereignty, we argue, would require domestic control over cloud infrastructure — not just local data centres — and clearer standards to distinguish genuine independence from marketing language.

[An episode of CBC’s Commotion](#) explored whether new age restrictions on tech platforms will protect kids — or just hand more power to the platforms themselves. As governments lean on companies to verify users, the episode raises a sovereignty question too: who decides how Canadians access digital spaces, and whose rules shape the public square online?

We were also quoted in a CBC story about [Big Tech’s growing market control and the risks of digital oligopolies](#) — and why this matters for Canada’s economic sovereignty. When a handful of global tech giants dictate the rules of engagement, the sovereignty of our digital, data, and economic architecture is at risk. It means higher barriers for new entrants, less leverage for local innovation, and diminished public policy space to steer outcomes.

Finally, some casual [tweets](#) and [Bluesky posts](#) about World Series tickets and resale markets catalyzed conversations with CBC’s The National (clip [here](#)) and Metro Morning, as well as a couple of print stories. The issue is a reminder that no application of technology is inevitable, and we have the power to create the markets we want.

This is a shimmering electro-pop track that feels like wandering through a neon-lit city and finding a secret door. On this single—part of her album *Jardin*—[MUNYA](#) fuses her Québécois roots with a sleek, global pop aesthetic.



SEND TO A FRIEND

