



Washington D.C. Can Legally Seize Canadian Data. Right Now.

No firewall stops it. No encryption key blocks it.

Legal jurisdiction is the attack surface — and a Canadian province has already written the Sovereign Intelligence standard that closes it.

Neil M. O'Connor — Sales Director, Banking and Financial Services, IAXOV

A Microsoft executive was asked under oath by a French Senate commission whether he could guarantee that data would not be transmitted to the US government without consent.[1]

His answer: “No, I cannot guarantee that.”

Read that again. Not a hacker. Not a breach. Not a ransom demand. The legal counsel of one of the world’s largest technology companies, under oath, confirming that if Washington asks for data his company holds, they will comply. Regardless of where the server is. Regardless of what your contract says. Regardless of Canadian law.

Right now, your bank’s AI models, your hospital’s patient records, your province’s tax filings, your employees’ health card numbers: if they are sitting on infrastructure operated by a US-domiciled company, a US government subpoena can reach them. Without your knowledge. Without your consent. Without violating a single law.

No firewall stops it. No encryption key blocks it. Legal jurisdiction is the attack surface. And we have been ignoring it for twenty-five years.



How We Got Here

In 2001, the United States passed the USA PATRIOT Act.[2] Section 215 gave US law enforcement authority to compel American companies to produce records held anywhere in the world. Canadians raised alarms. We kept signing contracts with American cloud providers anyway.

In 2018, the US passed the CLOUD Act.[3] It removed any remaining ambiguity. American companies must provide data stored anywhere in the world to US government authorities upon request. The server being in Canada is irrelevant. What matters is the vendor's legal domicile. And for the three American companies that control approximately 85% of Canada's cloud infrastructure spending, that legal domicile is Washington's jurisdiction.

In the second half of 2025 alone, Microsoft received 390 law enforcement requests involving Canadian accounts across criminal, civil, and emergency proceedings.[4a] Data was disclosed in response to the majority of them.[4b] Microsoft's own transparency reporting does not break out how many of those disclosures were compelled by US authorities under the CLOUD Act. That number is not publicly reported. Microsoft does not tell you when Washington is the one asking.

The autopsy of a disaster every Canadian institution is currently living in.

What Happens When the Blue Dye Hits the Pool

When a government employee sends a prompt containing a health card number to an AI tool running on US infrastructure, it is like dropping a single drop of blue dye into an enormous swimming pool.

You cannot reach in and pull it back out.

That data is absorbed. It is processed by a model operating under US legal jurisdiction. It informs training runs. It sits in logs that a US subpoena can reach. It cannot be extracted. It cannot be recalled. It is permanently beyond Canadian legal protection.

In 2025, Ontario's Auditor General found that approximately 12,000 Ontario Public Service employees accessed roughly 400 AI tools between April and August of that



year. Of those tools, 244 were rated unsafe or unsecured. Staff were uploading health card numbers, driver's licences, credit card information, and confidential government documents to platforms that feed US-operated AI systems.[5]

Twelve thousand Ontarians dropping blue dye into a pool operated by a foreign government's legal jurisdiction, every single day, one prompt at a time. Once it is in, it does not come back.

Now scale that to a Canadian bank's proprietary AI models. To a provincial hospital's patient database. To a federal department's classified procurement documents. In 2026, a geopolitical trade dispute is not a hypothetical. Imagine US authorities issuing a CLOUD Act demand for the AI-derived intelligence sitting in an American vendor's Canadian data centre. The Canadian institution cannot refuse. Their vendor's legal domicile in the US overrides Canadian privacy law. A hospital director explains to a patient why a foreign government has their medical file. A bank's board explains to its regulator why proprietary risk models are now accessible to Washington. They have no legal recourse. Their contract cannot protect them. Their data centre address cannot protect them. The only thing that could have protected them was never sending the data to a US-domiciled vendor in the first place.

What RBC Just Said Out Loud

In June 2026, RBC Thought Leadership published one of the most direct assessments of this problem I have read from a major Canadian financial institution.

The report is titled *Sovereign AI: Shaping Canada's Next Digital Chapter*. [6] Three US tech firms control approximately 85% of Canada's cloud infrastructure spending. Three more control roughly 88% of enterprise foundation model usage. Canada does not meaningfully participate in the global AI supply chain.

RBC frames sovereign AI not as protectionism but as freedom from coercion: the ability to choose which AI models to use, whose hardware runs AI inference, which jurisdiction governs data, and which providers can be substituted under pressure.

The stakes are concrete. With bank AI adoption rising from approximately 30% in 2019 to 50% in 2023 and projected to reach 70% by end of 2026, the procurement decisions Canadian banks make in the next twenty-four months may determine whether a



Canadian sovereign AI ecosystem reaches meaningful scale, or whether US vendors permanently consolidate their position in Canadian regulated sectors.

Procurement decisions made in the next twenty-four months will determine which side of that line Canada ends up on.

Alberta Already Showed Us the Standard

Earlier this year, the Government of Alberta issued Pre-Qualification Request TI-ITP-PQR-02-2026 for a Sovereign Compute Environment.[7] The Province did not accept a vendor's promise that a Canadian data centre made the exposure go away.

They required vendors to attest, in writing, under legal obligation, that neither they nor any subcontractor, officer, director, or employee was subject to any foreign law that could compel disclosure of data, access to systems, interception of communications, or assistance with intelligence or surveillance activities. The RFP named the laws specifically: the USA PATRIOT Act. The CLOUD Act. The Foreign Intelligence Surveillance Act. US National Security Letters. The UK Investigatory Powers Act. The Chinese National Intelligence Law.

That standard disqualifies IBM, Microsoft, Palantir, and every other US-domiciled AI vendor from the Province of Alberta's sovereign compute environment. Not because of where their servers are. Because of where their legal obligations sit.

A standard that already exists, in Canadian law, applied by a Canadian province. We do not need to invent anything. We need the will to apply it everywhere.

The Back Door Is Open. Here Is How to Close It.

For the Government of Canada

Ottawa released its national AI strategy, *AI for All*, on June 4, 2026,[8] with a "build-partner-buy" hierarchy that explicitly prioritizes Canadian-controlled infrastructure. That strategy means nothing until it becomes a procurement requirement.

Until Ottawa mandates the Alberta attestation standard for every federal AI contract, it is willingly leaving the back door open to foreign surveillance while publishing a strategy



that says sovereignty is a priority. The CUSMA Article 19.12 prohibition on mandating local compute facilities has no public policy exception.[9] The July 1, 2026, review milestone has now passed. Every federal AI contract signed without an attestation requirement is signed on the wrong side of it. The federal AI Source List has 73 pre-approved suppliers. Make it mandatory. Make sovereignty attestation the entry requirement. Every week without that requirement is another week of blue dye in the pool.

For the Province of Ontario

The Auditor General gave Ontario its mandate on May 12, 2026.[5] The Enhancing Digital Security and Trust Act gave Ontario its legal authority in January 2025.[10] The Information and Privacy Commissioner and Ontario Human Rights Commission gave Ontario its governance principles in January 2026.[11]

Until Ontario adopts the Alberta sovereignty attestation standard for all OPS AI procurement, the AG report is a public embarrassment without a remedy. Until Supply Ontario establishes a Vendor of Record listing for sovereign AI governance tooling, every ministry is running its own competitive process against a problem the province already diagnosed. The mandate exists. The legislation exists. The procurement mechanism is one decision away. Every month of delay is another twelve thousand employees dropping blue dye into a pool with a Washington address.

For Canadian Banks

Treating US vendor reliance as a routine IT procurement decision is a critical operational failure. In my direct engagements with federally regulated institutions, I have seen outsourcing risk analyses challenged specifically on foreign government access under the Bank Act's outsourcing provisions. A Canadian data centre commitment from a US vendor was not sufficient to satisfy that analysis. The CLOUD Act follows the company, not the server.

Update your outsourcing risk assessments to reflect CLOUD Act exposure before a foreign subpoena forces you to explain to Canadians why their money is safe, but their data is not. Require sovereignty attestation from AI vendors using the Alberta standard. And use your procurement power as anchor buyers. The sovereign ecosystem's viability depends on whether major financial institutions choose to use it. Every large AI governance contract awarded to a US-domiciled vendor on the basis of existing



relationships makes the Canadian sovereign ecosystem less viable. Every contract awarded to a Canadian-sovereign vendor makes it more viable. That choice is yours.

The Question That Closes the Conversation

Every institution, every government department, every bank, every hospital procurement team should be asking one question of every AI vendor:

Can you attest, in writing, under legal obligation, that no foreign government can compel access to our data?

If the answer is no, you do not have sovereign AI. You have a Toronto server address on a Washington-jurisdiction contract.

The Microsoft executive was honest about it under oath. The question is whether Canadian institutions will be as honest with themselves before Washington asks for the data, rather than after.

Neil M. O'Connor is Sales Director, Banking and Financial Services at IAXOV, a Calgary-based sovereign intelligence company. IAXOV builds LEGION, a patent-protected sovereign AI governance runtime deployed in production across Canadian government, banking, and not-for-profit sectors. Neil is the author of Strategic Revenue Enablement: The Tactical Execution of Your Go-to-Market Strategy (FriesenPress, 2026).



References

- 1.** Microsoft France. Director of Public and Legal Affairs. Testimony to the French Senate Commission of Inquiry on Digital Sovereignty. Paris: French Senate; 2025 Jun.
- 2.** United States. USA PATRIOT Act of 2001. Pub. L. No. 107-56, 115 Stat. 272. Washington (DC): US Government Publishing Office; 2001.
- 3.** United States. Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Pub. L. No. 115-141, 132 Stat. 348. Washington (DC): US Government Publishing Office; 2018.
- 4a.** Microsoft Global Affairs. Government Requests Report: Enterprise Disclosures to Law Enforcement, January to June 2025. Redmond (WA): Microsoft Corporation; 2025.
- 4b.** Microsoft Global Affairs. Law Enforcement Requests Report 2025: Requests Received for All Microsoft Services from July to December 2025. Redmond (WA): Microsoft Corporation; 2025.
- 5.** Ontario. Office of the Auditor General of Ontario. Special Report on Artificial Intelligence in the Ontario Public Service. Toronto (ON): Queen's Printer for Ontario; 2026 May 12.
- 6.** RBC Thought Leadership. Sovereign AI: Shaping Canada's Next Digital Chapter. Toronto (ON): Royal Bank of Canada; 2026 Jun 10.
- 7.** Government of Alberta. Pre-Qualification Request TI-ITP-PQR-02-2026: Sovereign Compute Environment. Edmonton (AB): Government of Alberta; 2026.
- 8.** Government of Canada. AI for All: Canada's National Artificial Intelligence Strategy. Ottawa (ON): Innovation, Science and Economic Development Canada; 2026 Jun 4.
- 9.** United States Trade Representative. 2026 National Trade Estimate Report on Foreign Trade Barriers. Washington (DC): Executive Office of the President; 2026 Mar.
- 10.** Ontario. Enhancing Digital Security and Trust Act, SO 2025. Toronto (ON): Queen's Printer for Ontario; 2025 Jan.
- 11.** Ontario Information and Privacy Commissioner; Ontario Human Rights Commission. Joint Statement on AI Governance Principles. Toronto (ON): IPC; 2026 Jan.