

'Everyone has woken up': Changing U. S. relationship propels Canada's data sovereignty into the spotlight

The Globe and Mail (Ottawa/Quebec Edition) · 27 Feb 2025 · B1 · JOE CASTALDO CASTALDO

Data sovereignty has long been a selling point for Craig McLellan's Toronto cloudcomputing company, ThinkOn Inc. But lately, the topic has come up a lot more often – and it has everything to do with Canada's damaged and uncertain relationship with the United States.



In this case, sovereignty means that data belonging to a Canadian entity is subject to the laws and regulations of this country, and cannot be easily accessed by a foreign government or law enforcement agency.

At ThinkOn, customers from the public and private sectors are asking a lot more questions about the security of their data and the reach of the U.S. Some have even asked for hard proof that their data is subject to the laws of Canada. "Everyone has woken up," Mr. McLellan said. "People are realizing that as long as that data is residing on a cloud infrastructure owned by an American company, they really aren't safe."

The reason for concern is U.S. President Donald Trump, who is threatening Canada with broad tariffs, talks about using "economic force" to compel the country into becoming the 51st state, and has installed loyalists at law enforcement agencies.

The President's coercive approach is prompting entrepreneurs, lawyers and other experts to consider how a U.S. administration could, if it wanted, strike at the heart of Canada's digital infrastructure, including cloud computing and artificial intelligence. Indeed, Canada's dependency on U.S. tech firms is another vulnerability that the White House can exploit. Canadian organizations rely heavily on U.S. companies such as Microsoft Corp., Google Inc. and Amazon.com Inc. for storing and managing proprietary data. Californiabased Nvidia Corp., meanwhile, is the world's biggest supplier of graphics processing units, or GPUs, the in-demand chips used to build and run AI models.

"Having a foreign supply of cloud compute puts our economic sovereignty at major risk," said Graham Dobson, a senior economist with the Dais think tank at Toronto Metropolitan University.

"From a data sovereignty perspective, that poses a far worse national security concern."

What once might have been outlandish scenarios are being discussed more seriously. Experts warn, for example, that the U. S. administration could put export controls on GPUs to Canada, hobbling the country's AI ambitions. They also fear a scenario in which the White House directs cloud providers to stop servicing Canadian clients, wreaking havoc on operations.

Barry Sookman, a senior counsel with McCarthy Tétrault LLP who focuses on technology and AI, suggests Canada should consider legal protections for that very scenario. "Could you have a law that makes it illegal for a subsidiary of a foreign company to carry out an executive order in the United States?" he said. "There could be some kind of legal infrastructure put in place to deal with that kind of emergency."

The tension with the U. S. has bolstered the case for building sovereign infrastructure here. But doing so is neither cheap nor quick, and in some cases, there are no easy alternatives. The hyperscalers, the term for cloudcomputing giants, have billions of dollars at their disposal and extensive operations. Overtaking them isn't realistic, according to Mr. McLellan. "We should find ways to complement them that allow us to minimize the risk," he said.

Concerns about data sovereignty have arisen before in Canada, particularly with the introduction of different pieces of U. S. legislation in the years after the 9/ 11 terrorist attacks – laws that beefed up the ability of authorities to compel data disclosure from American companies. Canadian organizations have responded in some cases by ensuring their data resides within Canadian borders. But that level of protection, known as data residency, may no longer be sufficient.

"Until recently, we weren't worried that the government was going to do something strange or punitive or for no reason," said Brent Arnold, a partner with Gowling WLG who specializes in cybersecurity. "We assumed if they were making requests for data, it would be for legitimate reasons."

At Calian Group in Ottawa, which provides cloud- management services, Mike Tremblay has been fielding more questions from clients on the topic lately, too. "We're spending a lot of time to help them understand how to protect themselves," said Mr. Tremblay, who is president of IT and cybersolutions. "If the FBI decides they want data, they can go to a U. S.- headquartered company and have them reach through their networks to that data that might even reside in Canada, and pull it out." In such cases, data could be accessed without the Canadian business even receiving any notification.

Cloud companies based outside the U. S. are also emphasizing their approach to data sovereignty. "We are the only hyperscaler that is able to commit to the fact that data won't be transferred to the United States," said Estelle Azemard, vice- president Americas at OVH- cloud, which is based in France and has two data centres in Canada, with plans to expand services. "That's important regarding what we are living with currently, the tension with the United States."

The actions of the U. S. Department of Government Efficiency, or DOGE, which is charged with finding cost savings, are another reason for concern. The effort has alarmed some security experts who warn DOGE has gained unprecedented access to sensitive data about Amer-

ican citizens. "The people making those decisions, I don't think they will have a moment's hesitation of saying, 'Well, go access Canadian data,'" said Robert Michon, a senior strategic adviser to Micrologic, a Quebec-based company that operates four data centres in Canada. Ottawa is aware of the importance of data sovereignty. A white paper from the Treasury Board of Canada Secretariat states that cloud providers with operations abroad could be required to comply with law enforcement requests for Canadian data, meaning sensitive information could be exposed to foreign governments. "Canada cannot ensure full sovereignty over its data when it stores data in the cloud," the paper states.

But the awareness hasn't always translated into action. "There's still a lot of education that needs to happen," Mr. Michon said. A recent cloud-computing tender from the federal government, for example, lists four pre-qualified bidders for the 25-year-long contract: all of them U. S. companies.

Inserting "Buy Canadian" requirements into these contracts would both improve data sovereignty and help grow domestic companies over time, said Stéphane Garneau, Micrologic's chief executive officer. "Everybody is looking around at what goods can be purchased locally. Well, the cloud is huge, huge, huge," he said.

Tensions with the U. S. could also affect Canada's goal of building more infrastructure to support AI. Last year, the federal government announced a sovereign AI compute program, dedicating \$ 700-million to build and expand data centres. Mr. Trump has already said he intends to put 25-per-cent tariffs on semiconductors, which could raise the prices of GPUs. But the disruption could go beyond that. The Biden administration blocked the export of AI chips to China, Russia, Iran and North Korea, and limited exports to a host of other countries, while exempting allies such as Canada.

The new U. S. administration could change its mind about exemptions in the future. "If Trump wants to cripple us, he just adds us to the list," Mr. Sookman said. "We're living in a time when the rules-based order is completely disintegrating."

The Canadian government has been building a relationship with Nvidia, but it's not clear what has become of these efforts. Last February, Innovation Minister FrançoisPhilippe Champagne said he and Nvidia CEO Jensen Huang had signed a letter of intent to explore opportunities for "creating AI computing power" in Canada, but otherwise offered no details. A spokesperson for Innovation, Science and Economic Development (ISED) did not provide any further information when asked for an update. The department could not provide a copy of the letter because it is deemed confidential, according to the spokesperson.

As for the sovereign AI infrastructure program, the federal government has made one funding announcement so far, allotting up to \$ 240-million to Cohere Inc. The money is a pre-purchase of capacity at a multibillion-dollar data centre that will be built in Canada by CoreWeave, an American company, using Nvidia GPUs.

The arrangement has been criticized by some experts who work in AI, given that Canadian federal funding ultimately flows to a U. S. company. "We are not using the money to create commercial stickiness for Canada. We're using the money to buy equipment with nothing

attached to it," said Hamid Arabzadeh, CEO of Ranovus Inc., an Ottawa company that makes hardware that integrates with AI chips to improve efficiency.

The funding between Cohere and ISED is not finalized, either, despite a splashy announcement by then deputy prime minister Chrystia Freeland at the company's Toronto headquarters in December.

The Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic at the University of Ottawa filed a freedom of information request for the funding agreement between ISED and Cohere, and was told in a Jan. 22 letter that the document did not exist because the two parties were still negotiating.

"Due diligence is taking place on Cohere's project and a contribution agreement will be signed following successful review and discussion," said Justin Simard, a spokesperson for ISED. Cohere declined to comment. As for Mr. McLellan, the heightened importance of data sovereignty could benefit ThinkOn in attracting new clientele. "We shouldn't really assume that any level of disruption is off the board," he said.