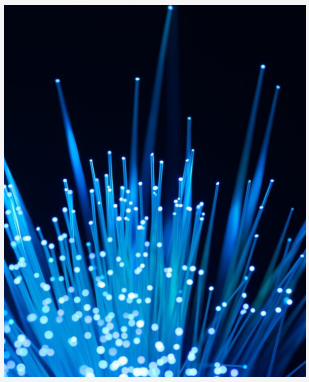
OSLER

Data sovereignty in light of the CLOUD Act: back to the future?

OCTOBER 7, 2025 12 MIN READ



Related Expertise

- Privacy and Data Management
- Technology

Authors: Michael Fekete, John Salloum

Ottawa and provincial governments across the country are facing demands for Canadians' data to be protected — in part — from foreign access under a U.S. law known as the CLOUD Act. These demands have become more pronounced in light of recent bilateral political developments and the reemergence as a high-profile issue of "data sovereignty" — that is, ensuring Canadian courts have exclusive authority over data within Canada's borders. Some commentators are similarly expressing concerns about the security of data stored with U.S. cloud providers, and the adoption of "sovereign cloud" solutions is increasingly being discussed at all levels of government.

These discussions are happening at a time when

- there are no documented cases of foreign government or law enforcement access to the data of Canadian enterprises processed within cloud services
- misconceptions about the CLOUD Act are common (for example, the CLOUD Act does not create surveillance powers or unfettered access to materials stored within cloud or other digital services in Canada)
- using a Canadian service provider or storing data in Canada does not guarantee data will be beyond the reach of courts in other countries
- a prominent attempt to mandate data sovereignty in British Columbia has been reversed
- it is increasingly clear that effective management of information in the digital age requires a risk-based approach that considers all relevant factors and costs, including the availability of technology-based solutions

This Update explores the prevalence of foreign access to electronic records stored in Canada, the impact of the CLOUD Act, and options for addressing related perceived risks.

Disclosures of enterprise customer content stored outside the U.S. is very low

Major cloud service providers regularly publish transparency reports that are designed to inform the public about the number and types of requests for user data they receive from

governments and courts worldwide, including the U.S. While these reports do not typically report on requests for data stored in Canada, the global numbers make it clear that the prevalence of disclosures of enterprise customer content stored outside the U.S. is very low.

What is the CLOUD Act?

The *Clarifying Lawful Overseas Use of Data Act* or CLOUD Act was enacted by the U.S. Congress in 2018 to modernize laws involving legal demands for information in the cloud computing era.

The CLOUD Act did not create *new* authority for U.S. law enforcement to obtain data. Instead, it applied traditional rules to electronic communication or cloud services providers under the jurisdiction of U.S. courts, including non-U.S. based companies that operate in the U.S. In doing so, the Act clarified that these service providers are required to comply with warrants for information stored outside the U.S. if the information is within the custody, control, or possession of the provider, while also maintaining common law comity protections. In other words, providers can challenge U.S. law enforcement demands for data under the CLOUD Act if doing so would violate another country's laws.

In addition, the CLOUD Act authorized the negotiation of reciprocal, bilateral agreements between the U.S. and foreign governments to allow law enforcement in both countries to reduce delays in cross-border requests for information by making requests directly to the service providers, instead of relying on mutual legal assistance treaties (MLATs) that could take months or even years. Canada has been negotiating a CLOUD Act agreement with the U.S. since 2022, but no agreement is currently in place. The negotiation was commenced as a product of the Cross-Border Crime Forum, an initiative to foster collaboration in fighting cybercrime, violent extremism and gun violence.

These powers are not new

Although the CLOUD Act has been criticized by some commentators as an example of extraterritorial overreach, many other countries have legal tools in place to enable domestic law enforcement investigating serious crimes to access electronic data stored in another country. In Canada, foreign corporations with a virtual presence in Canada have been compelled to produce data stored outside of Canada as part of a criminal investigation.[1] In the United Kingdom, the *Crime (Overseas Production Orders) Act* gives local law enforcement a mechanism for obtaining electronic data stored outside of the U.K. The e-Evidence Regulation in the European Union includes a similar process through which the court of an EU member state may order a cloud service provider in another EU member state to produce or preserve electronic evidence regardless of where the data is stored.

What is common among these laws, including the CLOUD Act, is they relate to criminal investigations within the jurisdiction of the local courts. In other words, they do not give law enforcement or foreign governments unrestricted access to information processed by service providers. Rather, they facilitate limited data collection in the context of criminal investigations when the provider is subject to the jurisdiction of the court.

Common misconceptions about the CLOUD Act

Misconception: The CLOUD Act created surveillance powers.

Reality: No surveillance powers were created. The CLOUD Act clarified existing U.S. legal process.

Misconception: The CLOUD Act allows the U.S. government or law enforcement to freely access information processed by cloud service providers in Canada.

Reality: Access to emails, documents or videos that Canadians create, communicate or store using cloud services requires a court-authorized warrant. A warrant requires establishing probable cause, based upon credible facts, of a criminal act within the jurisdiction of the U.S. Warrants are limited to the specific types of data identified in the warrant. Bulk data collection is not permitted. Non-content data, such as subscriber data, requires a court order, subpoena or similar legal process.

Misconception: The CLOUD Act allows the U.S. government to access trade secrets and other intellectual property processed by cloud service providers.

Reality: The CLOUD Act applies only to criminal investigations within the jurisdiction of the U.S. courts. Trade secrets and other intellectual property are very rarely relevant to a criminal investigation.

Misconception: The CLOUD Act requires a cloud service provider to develop backdoor access to stored data that has been encrypted.

Reality: The CLOUD Act does not require cloud service providers to decrypt information or prevent them from offering customer-controlled encryption or similar tools that remove the data from the provider's possession, custody, or control. It also prohibits the inclusion of a decryption mandate in a bilateral CLOUD Act agreement.[2]

Misconception: The CLOUD Act relies on a secretive judicial process.

Reality: Judicial warrants under the CLOUD Act are obtained through the pre-existing U.S. court process for criminal matters.

Misconception: The CLOUD Act provides no process for challenging a warrant if the request creates a conflict of law.

Reality: Common law "comity" challenges are preserved by the CLOUD Act.[3] This means that an application can be made to quash or modify a warrant on the basis that complying with it would conflict with another country's laws. It also provides additional grounds to challenge a warrant if a bilateral agreement is in place.

Misconception: Bilateral agreements authorized by the CLOUD Act undermine judicial protections.

Reality: A bilaterial agreement under the CLOUD Act is predicated on having privacy, human rights and rule of law protections in place.[4]

Storing data in Canada is no guarantee it will not be accessed

under foreign legal orders

Data processed in Canada by a foreign service provider or by a Canadian-owned service provider that has operations or representatives in a foreign country may be subject to legal orders outside Canada. For example, the CLOUD Act applies to any service provider that is subject to the jurisdiction of the U.S.[5] This means that U.S. law enforcement can serve legal process on the U.S. entity, compelling it to produce data, even if the data is held by a foreign parent or affiliate. The factual question for a U.S. court to consider is whether the service provider in the U.S. has "custody, control, or possession" over the data stored in another jurisdiction.

Key lessons from previous data sovereignty attempts in Canada

Twenty years ago, data sovereignty was a high-profile topic of discussion in Canada following the passing of the *U.S.A. PATRIOT Act*, together with the rapid adoption of cloud services. Legislative and regulatory responses also varied widely then. Provincial governments in British Columbia and Nova Scotia enacted strict data access and location laws applicable to personal information in the custody or control of public bodies. Alberta and Québec made relatively minor changes to their privacy laws, while most provinces made no changes.

The Office of the Privacy Commissioner of Canada published guidance that allows for personal information to be processed outside Canada where certain safeguards are in place, while the Treasury Board of Canada adopted a middle ground approach. In its Directive on Service and Digital, computing facilities located within Canada are identified as "a principal delivery option", but not the only option, for government-controlled electronic information categorized as Protected B, Protected C or Classified.

The focus on data sovereignty diminished over time, culminating in the Government of British Columbia amending its public sector privacy law in 2021 to remove the most restrictive elements of its data location and data access requirements. At the time, B.C. made clear it was changing its data residency rules "so public bodies can use modern tools while continuing to protect personal information."

Stated another way, the province essentially acknowledged that absolute data sovereignty is not achievable in an interconnected world, as it undercuts the ability of universities, schools, hospitals and government ministries to innovate, manage costs, and operate effectively. Ultimately, these requirements became unsustainable in light of the low likelihood of public sector data being the subject of an information demand by a foreign government.

Strategies for mitigating data sovereignty risks

Even if the risk is low, Canadian organizations need to understand what they can do to mitigate the possibility of data within their custody or control being subject to a foreign court order that is not subject to judicial oversight in Canada.

Using a Canadian-owned service provider

Using a Canadian-owned service provider that has no operations or representatives in the U.S. or another foreign country may be effective at achieving data sovereignty, assuming that the data is stored and can be accessed only in Canada. However, if the service provider has a presence in another country, such as subsidiaries, offices, employees, customers, or

infrastructure, it may be subject to the jurisdiction of the local courts. Furthermore, as was made clear in the B.C. government's experience with data residency rules, the availability of modern tools is limited.

Keeping data 'on-premise' in Canada

Processing an organization's data exclusively within its own premises and behind its own firewall is a second option. Doing so will likely insulate the data from foreign warrants if the organization is owned and controlled in Canada and has no foreign presence. However, maintaining on-premises infrastructure requires significant capital and investment in hardware, software, security, and skilled personnel, including to support backup and disaster recovery capacity. Moreover, on-premises solutions often lack scalability, flexibility, and access to the most advanced technologies, including cyber defences. For these reasons, on-premises solutions are increasingly reserved for processing only the most sensitive data, such as data implicating national security.

Implementing a 'sovereign cloud'

A "fully sovereign" public cloud solution would require data to be processed, transmitted and stored exclusively in Canada and always reman solely under the control of service providers that are not subject to foreign laws that permit access to data without the Canadian customer's consent.

The viability of a "fully sovereign" public cloud solution is questionable, as it would need to be delivered by a Canadian headquartered and controlled company with no meaningful presence outside Canada. This requirement would, in effect, require the creation and maintenance of a made-in and delivered-in-Canada solution by a provider without the experience, expertise, and funding gained by competing on the global market.

Recent experience in the EU highlights the challenges of developing a sovereign cloud. In 2019, an initiative known as GAIA-X was launched in Europe to reduce reliance on foreign cloud providers. Six years later, despite the investment of billions of Euros, GAIA-X has not achieved widespread market adoption, with many (if not most) organizations in Europe continuing to predominantly rely on global cloud service providers.

Leveraging technological solutions

Technology provides a range of options for maintaining control over data and mitigating or eliminating data sovereignty risks. Technology-based solutions, including the examples identified below, are likely to become more widely available over time, as service providers compete to win over and retain customers concerned about data sovereignty.

- **Encryption and key management**: Encrypting data at rest, in transit, and in use. When possible, organizations manage their own encryption keys (customer-managed keys) rather than relying on the encryption capabilities offered by the service provider.
- **Data access and identity management:** Deploying identity and access management systems to strictly control who can access data and from where, with monitoring and auditing of data access logs.
- **Data masking and tokenization:** Using data masking or tokenization to ensure that data remains unreadable without local de-tokenization or decryption.

- **Confidential computing**: Eliminating or reducing access to data while it is being processed by creating an isolated, hardware-based execution environment with a computer. Data processed with the environment remains invisible to the cloud provider.

Back to the future?

The reemergence of data sovereignty as a policy issue in Canada invites us to consider how governments and regulators across Canada will approach it in 2025 and beyond. The B.C. government's decision to amend its public sector privacy law in 2021 by removing the most restrictive elements of its data location and data access requirements provides some "lessons learned" that are equally relevant today. These lessons include the following:

- **Focus on actual risks:** Much of the public discussion concerning data sovereignty is drawn from fears of a foreign government compelling a cloud service provider to produce a customer's data even if it is stored in Canada. However, there is no evidence to suggest that this happens frequently.
- **Avoid a one-size-fits-all approach:** Consistent with data privacy laws, a risk-based approach to data sovereignty is needed. Strict on-premises data sovereignty safeguards may be appropriate for data that implicates national security or military operations, but applying these same safeguards to less sensitive information will often be disproportionate to the level of risk.
- **Account for all social and economic costs:** Building data centres in Canada may be the easy part of developing a "sovereign" solution. The more challenging — and costly — part may be sourcing sovereign products and services that will be deployed in them. Moreover, sovereign products and services are unlikely to offer the same range of productivity enhancing features as products and services available through the public cloud.
- **Recognize economic factors that make sovereign cloud solutions difficult to achieve.** Building domestic data centres provides no assurance that sovereign cloud solutions will flourish. Competing with established cloud service providers — who have been building their technology stacks for decades — makes the economics of sovereign cloud challenging. Moreover, procuring bespoke solutions that are unable to fully leverage commercially available software and infrastructure, can be expected to increase significantly the cost of a project, while reducing interoperability and resilience.

---

[1] *R v. Love, 2022 Alberta Court of Appeal 269* (leave to Supreme Court of Canada denied on April 20, 2023) and *Re Service de police de la Ville de Montréal*, 2022 QCCS 3935 (a decision of the Québec Superior Court)

[2] CLOUD Act, section 105(a).

[3] CLOUD Act, section 103(c).

[4] The U.S. Department of Justice has made this clear in a whitepaper: "*The CLOUD Act requires that the agreements include numerous provisions protecting privacy and civil liberties. Orders requesting data must be lawfully obtained under the domestic system of the country*

seeking the data; must target specific individuals or accounts; must have a reasonable justification based on articulable and credible facts, particularity, legality, and severity; and must be subject to review or oversight by an independent authority, such as a judge or magistrate. Bulk data collection is not permitted."

[5] CLOUD Act, section 102(2).