BSIA SPECIAL REPORT

BALSILLIE PAPERS

Whose Law Governs Canadian Data? The CLOUD Act, Executive Agreements and Digital Sovereignty

A Comprehensive Policy Briefing for Canadians

Barry Appleton

MARCH 11, 2026

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

1.1 The Core Problem

Canadian government data — including national defence communications — can be compelled by US authorities without Canadian judicial review or governmental notification. This is not a hypothetical risk. It is the operational reality created by the US Clarifying Lawful Overseas Use of Data or CLOUD Act of 2018.

When a senior Microsoft executive was asked under oath before the French Senate in June 2025 whether he could guarantee that French government data stored in Microsoft's cloud would never be transmitted to US authorities without French authorization, his answer was unequivocal: "*Non, je ne peux pas le garantir*" — "No, I cannot guarantee it."

The same is true for Canadian data.

1.2 Why This Matters Now

Over **80 percent of Canadian cloud services** rely on foreign infrastructure. Critical government systems — including the Department of National Defence's **Defence 365 platform** — depend on US-headquartered providers. Canada's largest telecommunications companies (Rogers, BCE, TELUS), financial services providers and technology firms maintain extensive US connections that expose them to CLOUD Act jurisdiction.

Storing data on Canadian soil does not protect it. The CLOUD Act compels disclosure based on who *controls* the data, not where it is stored. A US legal demand served on Microsoft, Amazon or Google requires compliance regardless of contractual commitments to Canadian customers or data residency arrangements.

Digital sovereignty, as used in this report, refers to the capacity of the Canadian government to exercise enforceable legal and constitutional control over data access, processing and disclosure. It does not depend on provider nationality or data residency alone. In principle, non-Canadian providers may form part of a sovereign digital ecosystem if — and only if — they are locally anchored in Canada, subject exclusively to Canadian law for data access purposes and insulated from conflicting extraterritorial legal obligations.

1.3 What Policymakers Should Understand

1.3.1 US Jurisdiction is Broader than Official Claims Suggest

The US Department of Justice asserts that CLOUD Act jurisdiction is "strictly constrained" by constitutional limits. This claim does not withstand scrutiny. Under the "national contacts" doctrine, US courts assess jurisdiction against a company's aggregate ties to the United States as a whole — not to any individual state. For Canadian companies with New York Stock Exchange (NYSE) listings, US institutional investors, American subsidiaries or US customers, the jurisdictional threshold is remarkably low.

BCE's August 2025 acquisition of Ziply Fiber — a US telecommunications company — transforms Canada's largest telecom into a North American operator almost certainly subject to CLOUD Act compulsion. TELUS operates in the US with 1,600+ US employees through TELUS Digital. Shopify processes 57 percent of its transactions in the United States and now lists New York as a principal executive office.

1.3.2 Corporate Assurances Cannot Override Legal Obligations

Microsoft's December 2025 announcement of C$19 billion in Canadian artificial intelligence (AI) investment came with pledges to challenge US legal orders and resist disclosure of Canadian data. These commitments are well-intentioned but legally insufficient.

The Bank of Nova Scotia legal cases from the 1980s established that US courts will enforce subpoenas against entities subject to US jurisdiction even when compliance violates foreign law — and will impose substantial fines for non-compliance. Microsoft's French Senate testimony confirmed what these precedents make clear: when a valid US legal demand arrives, US companies must comply.

1.3.3 Canadian and US Constitutional Standards are Fundamentally Incompatible

The Supreme Court of Canada has explicitly rejected the US "third-party doctrine." In *R v Spencer* (2014) and *R v Bykovets* (2024), the Court held that Canadians retain a reasonable expectation of privacy in electronic data held by service providers. The US constitutional framework reaches the opposite conclusion — enabling warrantless access to metadata and business records that Canadian law would protect.

A CLOUD Act agreement would allow US authorities to obtain Canadian data using legal standards that would be unconstitutional if applied in Canada.

1.3.3 Empirical Evidence from the UK Shows Executive Agreements Operate at Surveillance Scale

In 2024, the US Department of Justice confirmed that the United Kingdom issued over 20,000 direct requests to US providers in two years, overwhelmingly for interception, not for stored data — demonstrating that executive agreements normalize high-volume, secret surveillance outside mutual legal assistance treaty (MLAT) oversight. This represents persistent, programmatic access to large volumes of data without individualized judicial authorization.

1.3.5 The 2022 CLOUD Act Negotiations Should Be Suspended

What Canadians must understand is that Section 103 of the US CLOUD Act — authorizing unilateral extraterritorial compulsion — **is already operational**. US authorities can today demand Canadian data from any provider subject to US jurisdiction, without notification to affected Canadians and without Canadian judicial review. An executive agreement under Section 105 would not create this exposure; it would formalize and accelerate it while removing the MLAT's sovereignty layer entirely.

As The Citizen Lab's February 2025 analysis concluded: "One would be hard pressed to find two democracies that are more incompatible when it comes to trying to align digital surveillance laws."[1] Existing CLOUD Act agreements with the United Kingdom and Australia establish no rights or remedies for individuals whose data is seized — creating what researchers term a "remedial no-man's land."

A CLOUD Act agreement would *expand*, not limit, US jurisdictional assertions by providing consent under international law to extraterritorial enforcement.

1.3.6 The Broader US Policy Context is Concerning

The November 2025 US National Security Strategy declares that agreements with dependent allies "must be sole-source contracts for our companies"[2] and instructs Washington to "push out foreign companies that build infrastructure in the region."[3] The July 2025 White House AI Action Plan frames technological dominance — including "cloud dominance" — as a national security imperative.

These are not abstract policy positions. They are the context within which CLOUD Act powers will be deployed.

1.4 Policy Recommendations: A Seven-Pillar Framework

Canada possesses the legal authority and institutional capacity to respond. The question is whether there is political will to act. Section 12 of this report sets out detailed recommendations organized around seven pillars:

1. **Suspend CLOUD Act negotiations.** Halt executive agreement negotiations until constitutional compatibility is established and safeguards exceeding existing US-UK and US-Australia agreements can be guaranteed.
2. **Modernize blocking legislation.** Amend the Foreign Extraterritorial Measures Act to address digital data compulsion with sector-specific blocking orders, mandatory disclosure requirements and civil penalties.
3. **Migrate critical infrastructure.** Transfer national defence and security systems — including Defence 365 — to Canadian-controlled infrastructure not subject to US jurisdiction.
4. **Reform procurement policy.** Establish tiered sovereignty requirements for cloud procurements based on data sensitivity, with mandatory criteria for classified and protected information.
5. **Mandate encryption standards.** Require customer-controlled encryption for sensitive government data, ensuring providers cannot comply with foreign demands because they cannot access intelligible data.
6. **Invest in MLAT capacity.** Address processing delays through institutional investment rather than sovereignty bypass, preserving Canadian judicial oversight of foreign data requests.
7. **Establish private sector transparency.** Create disclosure obligations for telecommunications and critical infrastructure providers regarding CLOUD Act exposure and compliance with foreign legal demands.

These are not abstract policy positions. They are the context within which CLOUD Act powers will be deployed.

1.5 The Choice before Canada

The decisions policymakers make in the coming months — on CLOUD Act negotiations, on critical infrastructure procurement, on encryption standards — will determine whether Canada retains meaningful sovereignty over its digital domain.

The alternative is accepting foreign surveillance of Canadians — data compelled without notification, without due process and without Canadian judicial oversight — as the operational norm. The Canadian data is ultimately subject to the legal process of a foreign jurisdiction whose constitutional framework operates on fundamentally different principles than our own. That is not a trade-off. It is nothing less than a surrender.

2. DECISION LOGIC FOR CANADIAN POLICYHOLDERS

The CLOUD Act presents Canadian policymakers with a fundamental choice between two governance models. The consequences of that choice extend far beyond operational efficiency.

Table 1: Two Governance Paths

Path A: Executive Agreement	Path B: Sovereign Controls + MLAT
Access Model Direct foreign access to Canadian data via providers	**Access Model** Foreign requests processed through Canadian authorities under Canadian law
Judicial Oversight No Canadian judicial gatekeeping	**Judicial Oversight** Canadian courts review foreign requests under Charter standards
Operational Scale Normalizes high-volume, interception-scale requests (20,000+ annually under UK agreement)	**Operational Scale** Maintains deliberate process; serious crimes prioritized through existing channels
Constitutional Alignment Accepts US third-party doctrine incompatible with Canadian *Spencer/Bykovets* decisions	**Constitutional Alignment** Preserves privacy protections for Charter-protected persons whose data is subject to protection under section 8 of the Charter
Trade-off Gains marginal processing speed; surrenders constitutional control	**Trade-off** Requires capacity investment; maintains sovereignty and bargaining leverage

2.1 The Core Question

Which constitutional order will govern Canadian data — Canadian law applied by Canadian courts or US law applied by US authorities without Canadian oversight?

Three threshold questions for any policy decision:

- **Jurisdictional exposure:** is the provider or system subject to US legal compulsion? (If uncertain, assume yes.)
- **Data sensitivity:** would unauthorized disclosure engage Charter-protected interests, including national security, section 8 privacy rights, section 7 security-of-the-person and due-process interests, section 15 equality concerns or democratic governance more broadly?
- **Technical protection:** can data be rendered inaccessible to the provider through customer-controlled encryption?

If jurisdictional exposure exists and data sensitivity is high, Canadian-controlled alternatives or robust technical protections are required — regardless of contractual assurances or data residency arrangements.

Section 12 below provides detailed recommendations for implementing this framework across seven policy domains.

3. UNDERSTANDING THE US CLOUD ACT

3.1 What is the CLOUD Act?

The CLOUD Act is a US federal law enacted on March 23, 2018, as part of the Consolidated Appropriations Act.[4] The CLOUD Act fundamentally expanded the extraterritorial reach of US law enforcement by clarifying that US legal process can compel the production of electronic data, regardless of where it is physically stored — including data stored on servers located in Canada or any other foreign country.

The core statutory provision, codified at 18 U.S.C. § 2713, provides that a covered provider "shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's **possession, custody, or control**, [author's emphasis] regardless of whether such communication, record or other information is located within or outside of the United States."

3.2 Entities Subject to CLOUD Act Jurisdiction

The CLOUD Act applies to two categories of service providers defined in the Stored Communications Act:[5]

- **Electronic Communication Service (ECS):** Defined under 18 U.S.C. § 2510(15) as "any service which provides to users thereof the ability to send or receive wire or electronic communications." This includes email providers, messaging services, telecommunications companies and social media platforms. The CLOUD Act covers electronic communications and associated electronic data, including both content and non-content information.
- **Remote Computing Service (RCS):** Defined under 18 U.S.C. § 2711(2) as "the provision to the public of computer storage or processing services by means of an electronic communications system." This encompasses cloud storage providers, data processing services, hosting platforms and software-as-a-service providers. Entities that provide secure message-hosting services, such as insurers and financial institutions, fall within the broad RCS definition.

The jurisdictional reach is remarkably broad. Unlike some US regulatory frameworks — such as the Office of Foreign Assets Control economic sanctions programs, which focus primarily on transactions involving US persons, US dollar clearing or entities with a specific US nexus — the CLOUD Act asserts jurisdiction over **any provider subject to US jurisdiction**, regardless of where the provider is headquartered or where its data is stored.

3.3 Canadian Government and Critical Infrastructure Exposure

The CLOUD Act does not itself confer jurisdiction; it operates once US courts determine that jurisdiction exists under ordinary constitutional principles. However, the scope of Canadian exposure to CLOUD Act jurisdiction is extensive.

According to the Canadian government, over 80 percent of Canadian cloud services rely on foreign infrastructure.[6] This creates systemic dependency on providers subject to foreign legal process.

Particularly concerning is the exposure of critical government systems. The Department of National Defence (DND) and Canadian Armed Forces (CAF) make significant use of Microsoft 365 through their defence-tailored product called Defence 365, which serves as a common cloud infrastructure for collaboration across DND/CAF, with stakeholders and other government departments.[7] Under current arrangements, any data on these systems could, in theory, be subpoenaed by US authorities without Canadian judicial review.

As the Privacy Commissioner of Canada noted in the 2023-2024 annual report, "data residency requirements alone cannot guarantee protection from foreign legal processes."[8] Microsoft's subsequent admission before the French Senate confirmed this assessment. The policy implications of this exposure are addressed below in Section 12.

3.4 How Can the CLOUD Act Apply to Canadian Data?

The CLOUD Act applies to Canadian data through multiple pathways:

- **Direct application to US-headquartered providers:** When Canadians use services provided by US-headquartered companies — Microsoft, Google, Amazon Web Services, Apple, Meta or others — their data is subject to CLOUD Act jurisdiction regardless of where it is physically stored.
- **Application through corporate control:** The CLOUD Act's "possession, custody or control" language extends its reach to data held by foreign subsidiaries of US companies.[9]
- **Application to foreign companies with US presence:** The CLOUD Act is not limited to US-headquartered companies. Any provider of electronic communication services or remote computing services that is subject to US jurisdiction can be compelled to produce data. A company is subject to US jurisdiction if it has "minimum contacts" with the United States — a standard discussed in detail in section 4.1 below.[10]
- **Application through network transit and routing infrastructure:** CLOUD Act exposure is not limited to data at rest with a provider. Canadian data may also be exposed during transit when it is

routed through US network infrastructure — even when both the sender and recipient are located in Canada. Research on Canadian internet routing patterns has documented that a significant proportion of domestic Canadian internet traffic "boomerangs" through US network exchange points or travels over US-controlled fibre routes before returning to Canadian endpoints, sometimes without the knowledge of the data's owner.[11] Because the CLOUD Act's "electronic communication service" definition encompasses providers that facilitate the transmission of electronic communications, data in transit through US-based or US-controlled network infrastructure may be interceptable under US legal authority regardless of its Canadian origin and destination. This network-layer vulnerability underscores why data sovereignty cannot be achieved through storage-location requirements alone; genuine protection requires what scholars and practitioners increasingly term "full-stack sovereignty" — control not only over data storage but over the computer, networking and routing infrastructure through which data flows.[12]

3.5 What "Sovereign Cloud" Means for Canadian Policy

For the purposes of Canadian digital sovereignty, a "sovereign cloud" is not defined by server location alone. Data residency is a necessary but insufficient condition.

A cloud service qualifies as "sovereign" only where Canada retains effective control across four dimensions:

- **Jurisdictional control:** the provider and relevant operating entities are not subject to foreign legal regimes that can compel disclosure of Canadian data without Canadian authorization.
- **Operational control:** day-to-day administrative access, system management and security operations are exercised by entities accountable under Canadian law, without unilateral override by foreign parent companies.
- **Cryptographic control:** encryption keys for sensitive data are held by Canadian customers or Canadian authorities, not by providers subject to foreign compulsion.
- **Audit and enforcement authority:** Canadian institutions possess meaningful audit rights, transparency mechanisms, and enforcement tools to verify compliance and respond to foreign legal demands.

Cloud offerings that rely solely on Canadian data centres, contractual assurances or voluntary corporate commitments — while preserving foreign jurisdictional exposure or provider-held keys — do not meet this standard.

In short: **sovereignty is about control, not geographic coordinates.**

4. US PERSONAL JURISDICTION DOCTRINE: WHAT CANADIANS NEED TO KNOW

A critical issue for Canadian policymakers is understanding how US courts determine whether a foreign entity — including a Canadian company — is subject to US jurisdiction for CLOUD Act purposes. The US constitutional framework governing personal jurisdiction operates on principles largely unfamiliar to Canadian lawyers, and the US government's official position on jurisdictional constraints may significantly overstate the protections available to foreign service providers.

4.1 The "Minimum Contacts" Test

Under US constitutional law, the Due Process Clause of the Fifth Amendment (for federal process) and the Fourteenth Amendment (for state process) limit a court's authority to exercise jurisdiction over a defendant. The foundational case is *International Shoe Co. v Washington* (1945), which held that due process requires a defendant to have "minimum contacts" with the forum such that the exercise of jurisdiction does not offend "traditional notions of fair play and substantial justice."[13]

The minimum contacts analysis has evolved through subsequent Supreme Court decisions into a doctrine of "purposeful availment" — the requirement that a defendant has "purposefully avail[ed] itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws."[14] For internet-era service providers, courts have applied variations of this test, including the "*Zippo* sliding scale" for assessing web-based contacts[15] and in appropriate cases, the "*Calder* effects test" for intentional conduct directed at forum residents.[16] In the CLOUD Act context, these jurisdictional tests matter because they help determine whether a foreign-based service provider's online operations — such as interactive services, targeted content or intentional engagement with US users — are sufficient to establish US personal jurisdiction, thereby subjecting the provider to compulsory US legal process for data within its possession, custody or control, regardless of where that data is stored.

Applying these principles, t**he practical implications for Canadian companies are significant**. A Canadian company that offers electronic communication services or remote computing services to persons in the United States — even without physical presence in the United States — **may, depending on the totality of circumstances, establish sufficient "minimum contacts" with the United States**,[17] through a range of ordinary commercial and digital activities.

These may include maintaining ongoing commercial relationships with US customers;[18] repeatedly routing transactions through US-based financial infrastructure or correspondent banking systems;[19] targeting advertising or marketing to US markets;[20] entering into contracts governed by US law or that deliberately affiliate the company with US legal protections and obligations;[21] or hosting online content or services that are intentionally directed at, and monetized from, US audiences.[22] In the aggregate, such contacts

may be sufficient to support the exercise of US personal jurisdiction over a foreign service provider notwithstanding the absence of any physical presence in the United States.[23]

4.2 Federal "National Contacts" Doctrine and CLOUD Act Exposure

In federal-question cases arising under statutes that authorize nationwide or worldwide service of process, US courts have long held that the relevant inquiry under the Fifth Amendment Due Process Clause is whether the defendant has sufficient contacts with the *United States as a whole*, rather than with any particular state.[24] This "national contacts" approach reflects the principle that, where Congress legislates on matters of national scope, personal jurisdiction analysis is anchored to the sovereign reach of the United States itself.[25]

Courts applying this framework have emphasized that Fifth Amendment due process imposes a general fairness inquiry incorporating the familiar *International Shoe* standard, but assessed against aggregate US contacts and with fewer territorial constraints than apply under the Fourteenth Amendment.[26] As a result, foreign defendants may be subject to US federal jurisdiction even where their contacts with any single state would be insufficient, provided that their overall US contacts demonstrate purposeful availment of the US market or legal order.[27]

This doctrine is directly relevant to the CLOUD Act. The Stored Communications Act, as amended, is a federal statutory regime enforced through federal courts, and the CLOUD Act compulsion operates only once a provider is subject to US federal jurisdiction. In that context, even relatively modest but deliberate engagement with US users, infrastructure or markets may satisfy Fifth Amendment due process when assessed on a national-contacts basis, thereby exposing foreign service providers to compulsory US legal process for data within their possession, custody or control.[28]

4.3 The Fifth Amendment Due Process Does Not Meaningfully Constrain CLOUD Act Jurisdiction

US government statements asserting that the CLOUD Act is "strictly constrained"[29] by Fifth Amendment due process protections substantially overstate the practical limits those protections impose. In federal-question cases governed by nationwide service of process, courts have long applied a national-contacts framework under which due process is satisfied so long as the defendant has sufficient aggregate contacts with the United States as a whole, assessed through a generalized fairness inquiry.[30] This approach affords Congress wide latitude to extend federal jurisdiction[31] and imposes significantly fewer territorial constraints than the state-based Fourteenth Amendment analysis familiar to Canadian lawyers.[32]

As multiple courts and commentators have observed, Fifth Amendment due process in this context

functions less as a robust jurisdictional barrier than as a minimal reasonableness check, one that is rarely dispositive where a foreign entity has deliberately engaged with US markets, users or infrastructure.[33] The result is that constitutional "constraints" invoked by the US Department of Justice do not operate as meaningful safeguards against CLOUD Act compulsion for foreign service providers with routine US commercial or digital ties.[34]

Reliance on these constraints, therefore, provides little practical protection for Canadian data, particularly where the provider falls within the Stored Communications Act's definitions of electronic communication service or remote computing service and maintains ongoing engagement with the United States.[35]

4.3.1. Why Due Process Constraints Are Illusory

The US Department of Justice has officially asserted that the CLOUD Act does not expand US jurisdiction and that personal jurisdiction over foreign providers is "strictly constrained by the personal jurisdiction requirement contained within the Constitution's Fifth Amendment Due Process Clause."[36] This position — that constitutional protections meaningfully limit CLOUD Act assertions over foreign service providers — has been forcefully challenged by legal scholars.

Tim Cochrane's analysis in the *Duke Journal of Comparative & International Law* argues that this official position is misleading. Cochrane demonstrates that "it is seriously questionable whether the Due Process Clause imposes any meaningful restrictions" in the CLOUD Act context.[37] His analysis identifies several reasons why Canadian policymakers should not rely on US constitutional constraints to protect Canadian data:

- First, CLOUD Act executive agreements expand enforcement jurisdiction at public international law. When a foreign state enters a CLOUD Act agreement with the United States, it "consents" (in international law terms) to US assertions of jurisdiction over its territory. This consent significantly weakens any comity-based challenges and removes one of the few practical obstacles to extraterritorial enforcement.[38]
- Second, Congress possesses broad authority to extend federal courts' personal jurisdiction. Constitutional scholar Stephen Sachs has argued that "Congress can extend the federal courts' personal jurisdiction as far as it wants."[39] While the Supreme Court has recently *narrowed* personal jurisdiction in some contexts,[40] these limitations apply primarily to *general* jurisdiction (requiring a defendant be "at home" in the forum) rather than *specific* jurisdiction arising from targeted conduct.
- Third, it remains unclear whether foreign persons and entities are entitled to Fifth Amendment due process protections at all. The Supreme Court's extraterritorial jurisprudence — including cases involving Guantanamo detainees — suggests a context-specific, functional analysis rather than automatic extension of constitutional protections to non-citizens abroad.[41]

4.4 Third-Country Interception Authority

A further dimension of CLOUD Act exposure concerns interception of communications involving persons located in neither the requesting nor the receiving state. Legal scholars have identified what Albert Gidari termed "the big interception flaw" in CLOUD Act agreements: they permit either party to require a covered provider to intercept the communications of users located in third countries "without the approval of that sovereign nation and perhaps even without its knowledge."[42]

Under US law, an "interception" occurs where communications are heard (the "listening post"), where the target device is located or where interception equipment diverts communications.[43] This means a UK wiretap order served on a US provider could lawfully intercept communications of a Canadian user without Canadian authorization — provided the communications were routed through US-based infrastructure and "listened to" by UK authorities.

For Canada, this raises a troubling prospect: even absent a Canada-US CLOUD Act agreement, Canadian communications may already be subject to foreign interception through CLOUD Act mechanisms that bypass the Canadian legal process entirely.

4.5 "*International Shoe*'s Days May Be Numbered"

Perhaps most concerning for foreign entities relying on US constitutional constraints is that the International Shoe framework itself has been questioned by sitting Supreme Court Justices. In *Ford Motor Co. v Montana Eighth Judicial District Court* (2021), Justice Gorsuch's concurrence questioned whether the International Shoe approach remains appropriate for modern commerce, and Justice Alito asked, "whether the case law we have developed... is well suited for the way in which business is now conducted."[44]

As Cochrane observes, these judicial reservations suggest that "*International Shoe*'s days may be numbered."[45] For Canadian policymakers, this means that even the existing — already limited — constitutional framework for jurisdictional analysis may evolve in ways that further expand US extraterritorial reach into companies that operate in Canada but have some incidental US connections.

4.6 Implications for Canadian Service Providers

Canadian telecommunications providers (Rogers, Bell, TELUS), financial and banking providers, technology companies (Shopify) and financial institutions with US business contacts should understand that:

- Any service offering that falls within the Stored Communications Act's definitions of ECS or RCS may be subject to CLOUD Act compulsion if the provider has sufficient US contacts.

- US constitutional protections, including the Fifth Amendment Due Process Clause, may not meaningfully constrain US jurisdiction over Canadian providers.
- A Canada-US CLOUD Act executive agreement — currently under negotiation — would expand rather than limit US jurisdictional assertions by removing public international law obstacles to extraterritorial enforcement.
- Companies should conduct jurisdiction-specific risk assessments and consider operational structures that minimize US jurisdictional exposure, including customer-controlled encryption that limits the provider's ability to comply with disclosure demands.

4.7 Case Studies: Canadian Telecommunications and Technology Companies

The abstract principles of US personal jurisdiction doctrine have concrete implications for major Canadian telecommunications and technology companies. This section examines specific US connections that may subject Canada's largest service providers to CLOUD Act compulsion.

4.7.1 US Stock Exchange Listings and Institutional Ownership

Canada's three largest telecommunications providers — Rogers Communications, BCE Inc. and TELUS Corporation — are all dual listed on US stock exchanges, a factor that creates multiple potential bases for US personal jurisdiction.

Table 2: Canadian Telecommunications Providers with US Ownership

Company	US Listing	US Institutional Ownership	SEC Filing Obligations
Rogers Communications	NYSE: RCI	~45% US institutional shareholders[46]	Form 20-F; subject to US securities law
BCE Inc.	NYSE: BCE	Significant US institutional investors[47]	Form 20-F; subject to US securities law
TELUS Corporation	NYSE: TU	Significant US institutional investors[48]	Form 20-F; subject to US securities law

Data compiled by the author from publicly available corporate disclosures, including SEC filings, company annual reports, investor materials, and stock exchange records.

Dual listing on US exchanges creates a substantial nexus with the United States that goes well beyond passive market exposure. These companies:

- **Submit to Securities and Exchange Commission (SEC) jurisdiction**: By listing on US exchanges, Canadian telecommunications providers voluntarily submit to the regulatory jurisdiction of the US SEC, accepting obligations under US securities law, including the Securities Exchange Act of 1934 and the Sarbanes-Oxley Act of 2002.
- **Engage US financial infrastructure**: Dual-listed companies routinely conduct transactions through US dollar clearing systems and correspondent banking relationships, factors that US courts have found sufficient to establish purposeful availment.[49]
- **Cultivate US investor relationships**: Through investor roadshows, analyst calls, and shareholder communications directed at US institutional investors, these companies deliberately affiliate themselves with US capital markets.
- **Enter contracts governed by US law**: Bond indentures, credit facilities and other financing arrangements frequently incorporate New York law choice-of-law provisions and submission to New York court jurisdiction.

Under the "purposeful availment" doctrine articulated in *Burger King Corp. v Rudzewicz*,[50] such deliberate engagement with US markets and legal frameworks may constitute sufficient "minimum contacts" to support personal jurisdiction — particularly when assessed on an aggregate, national-contacts basis under Fifth Amendment due process analysis.

4.7.2 Direct US Operations and Subsidiaries

Beyond securities listings, major Canadian telecommunications providers maintain direct operational presence in the United States through subsidiaries and acquisitions.

BCE Inc. / Bell Canada

In August 2025, BCE completed its acquisition of Ziply Fiber, a US telecommunications company operating in the states of Washington, Oregon, Idaho and Montana, for approximately C$5 billion.[51] Ziply Fiber operates as a wholly owned subsidiary of BCE and provides fiber-optic internet services to residential and business customers across the Pacific Northwest.

This acquisition transforms BCE from a purely Canadian telecommunications provider into a North American operator with direct US presence. BCE now:

- Operates US telecommunications infrastructure
- Employs US personnel
- Serves US customers directly
- Maintains US business records and customer data

For CLOUD Act purposes, this operational footprint almost certainly satisfies personal jurisdiction requirements. BCE is no longer merely a Canadian company with US investor contacts; it is now a provider of electronic communications services to US customers through US-based infrastructure.

TELUS Corporation

TELUS operates extensive US operations through TELUS Digital (formerly TELUS International), which maintained dual listings on both the NYSE and Toronto Stock Exchange until TELUS acquired the remaining public shares in September 2025.[52] TELUS Digital's US presence includes:

- **TELUS International (US) Corp.**: A US subsidiary headquartered in Las Vegas, Nevada, with over 1,600 employees.[53]
- **Gerent**: A US-based Salesforce consultancy acquired in May 2025.[54]
- **Multiple US client service operations**: TELUS Digital provides digital customer experience services to major US technology companies

TELUS Digital's business involves precisely the types of services — digital customer experience, data processing and AI data annotation — that fall within the Stored Communications Act's definitions of electronic communication services and remote computing services.

Rogers Communications

While Rogers does not maintain the same direct US operational presence as BCE or TELUS, its NYSE listing, substantial US institutional ownership (approximately 45 percent of outstanding shares),[55] and ongoing commercial relationships with US content providers, equipment manufacturers and financial institutions create significant jurisdictional exposure.

4.7.3 Canadian Technology Companies: The Shopify Example

The CLOUD Act's jurisdictional reach extends beyond traditional telecommunications providers to any company offering "electronic communication services" or "remote computing services.: Canadian technology companies with substantial US connections face analogous exposure.

Shopify Inc. provides a particularly instructive example. The Ottawa-headquartered e-commerce platform:

- **Transferred its US listing from the NYSE to NASDAQ** in March 2025, becoming a component of the NASDAQ-100 index[56]
- **Processes the majority of its transactions in the United States** — 57 percent of Shopify's US$292.3 billion in 2024 gross merchandise volume was processed in the United States[57]

- **Maintains US offices**, including operations in San Francisco and New York with approximately 900 combined employees[58]
- **Operates US subsidiaries**, including Shopify Data Processing (USA) Inc. and Shopify Holdings (USA) 2 Inc.[59]
- **Filed a 10-K domestic issuer form** in February 2025 listing New York as a "principal executive office" alongside Ottawa, with the majority of segmented assets now reported as located in the United States[60]

Shopify's platform enables millions of merchants to process payments, communicate with customers and store transaction data — activities that squarely fall within the Stored Communications Act's definition of remote computing services. A US legal demand served on Shopify could theoretically compel production of merchant and customer data regardless of where that data is stored.

4.7.4 Jurisdictional Implications

The US connections documented above have significant implications for Canadian data sovereignty.

1. Multiple Jurisdictional Hooks

Each company presents multiple independent bases for US personal jurisdiction:

Table 3: Jurisdictional Factors

Jurisdictional Factor	Rogers	BCE	TELUS	Shopify
U.S. stock exchange listing	✓	✓	✓	✓
U.S. institutional investors	✓	✓	✓	✓
U.S. subsidiaries	—	✓	✓	✓
U.S. employees	—	✓	✓	✓
U.S. customers served directly	—	✓	✓	✓
SEC reporting obligations	✓	✓	✓	✓

Data compiled by the author from publicly available corporate disclosures and legal sources, including corporate filings, company reports, and publicly documented information on U.S. listings, subsidiaries, operations, and investor ownership.

2. Aggregate National Contacts

Under the Fifth Amendment national-contacts framework applicable to federal statutory cases like

CLOUD Act compulsion, these connections are assessed in the aggregate against the United States as a whole — not against any individual state.[61] This substantially lowers the jurisdictional threshold compared to state-court analysis under the Fourteenth Amendment.

3. "Possession, Custody or Control" Extends to Subsidiaries

The CLOUD Act's "possession, custody or control" language means that data held by Canadian parent companies may be reachable through their US subsidiaries, and vice versa. US courts have consistently held that corporate separateness does not defeat compelled disclosure where the entity served with process has practical ability to obtain the data.[62]

4. Electronic Communication Services and Remote Computing Services

All four companies examined provide services that fall within the Stored Communications Act's jurisdictional definitions:

- **Rogers, BCE, TELUS**: As telecommunications providers, they offer "electronic communication services" including mobile messaging, email and voice services.
- **Shopify**: As a cloud platform, it provides "remote computing services" including data storage and processing.
- **TELUS Digital**: Its customer experience and data annotation services involve processing and storing electronic communications on behalf of clients.

4.7.5 Practical Consequences for Canadian Data

The jurisdictional exposure documented above means that:

1. **Customer data held by Canadian telecommunications providers may be subject to CLOUD Act compulsion** regardless of where that data is physically stored, if the provider is subject to US personal jurisdiction.
2. **Data localization provides limited protection** when the cloud provider or telecommunications company remains subject to US jurisdiction through stock listings, subsidiaries or commercial relationships.
3. **Corporate assurances of data sovereignty cannot override legal obligations**: As Microsoft's June 2025 French Senate testimony confirmed,[63] companies subject to US jurisdiction must comply with validly served US legal process regardless of contractual commitments to foreign customers.
4. **Canadian judicial oversight may be bypassed entirely**: Under current law, US authorities can obtain Canadian telecommunications data directly from US-affiliated providers without any involvement of Canadian courts or governmental authorities.

5. LEGISLATIVE FRAMEWORK

5.1 Background: The Microsoft Ireland Case

The CLOUD Act emerged from *United States v Microsoft Corp.* (2018), where Microsoft challenged a US warrant seeking customer emails stored on servers in Ireland.[64] Before the Supreme Court could rule, Congress passed the CLOUD Act, mooting the case while clarifying US law enforcement's authority to compel production of data regardless of storage location.

5.2 Relationship to the Canada-US MLAT

The Canada-United States MLAT embodies a constitutional allocation of investigative authority. Foreign law enforcement officials do not exercise coercive powers within Canada. Instead, requests for evidence located in Canada are routed through Canadian public authorities and, where required, Canadian courts applying Canadian law and Charter standards.[65]

The significance of the MLAT framework is not efficiency but institutional control. The point at which compulsion occurs — the issuance and execution of a production order or warrant — is an act of Canadian legal authority. This ensures democratic accountability, judicial supervision, proportionality review and compatibility with Canadian constitutional norms.[66]

CLOUD Act-style "direct-to-provider" mechanisms do not modernize this framework. They displace it. By allowing foreign legal process to be executed through private intermediaries subject to foreign jurisdiction, such mechanisms reroute coercive authority away from Canadian institutions and into a foreign constitutional order that Canada has explicitly declined to adopt.[67]

5.2.1 How MLAT Requests Work in Practice: The Normal "Foreign Request" Pathway

Before any CLOUD-style direct-to-provider system, the default method for foreign law enforcement to obtain evidence in Canada is **mutual legal assistance (MLA/MLAT)**. The core point is not speed; it is **institutional control**: MLATs force foreign demands for evidence in Canada to pass through **Canadian public authorities and (where required) Canadian courts**.

A simplified MLAT workflow (Canada–US) looks like this:

1. **Foreign authority prepares the request** (for example, US investigators identify a target account, device identifier, subscriber data, content or intercept assistance).
2. **Request is transmitted government-to-government** to Canada's **Central Authority** (federal officials responsible for MLAT administration).

3. **Canadian officials review the request** for legal sufficiency and compatibility with Canadian law, including proportionality, Charter risk and whether the request is appropriately scoped.
4. **4.Canadian legal process is obtained where needed** (for example, production order/warrant under Canadian law). This step is the **sovereignty hinge**: the coercive act occurs through **Canadian legal authority**, not a foreign process.
5. **Evidence is collected in Canada** (from providers or custodians) under Canadian legal constraints, including applicable notice/gag rules, minimization and judicial supervision where required.
6. **Evidence is transmitted back** to the requesting state, typically with **conditions** on use, onward disclosure, and compliance undertakings.

Why this matters: MLATs embed the principle that **foreign police do not execute investigative powers inside Canada without Canadian oversight**. A CLOUD-style bypass mechanism shifts that baseline by allowing requests to land on providers (or corporate parents) without Canadian institutional involvement — functionally converting Canadian territory into a **foreign evidence reservoir** governed by foreign legal standards.

5.3 Two Core Mechanisms

The CLOUD Act operates through two distinct but cumulative mechanisms — one unilateral and already in force, the other bilateral and contingent on negotiation.

5.3.1 Extraterritorial Compulsion (Section 103)

Section 103 of the CLOUD Act clarifies that US legal process under the Stored Communications Act applies to data within a provider's "possession, custody, or control," regardless of where the data is physically stored.[68] This authority is fully operational. US authorities may compel production of Canadian data from any provider subject to US jurisdiction without Canadian notification, without Canadian judicial authorization, and without any bilateral agreement.

5.3.2 Executive Agreement Framework (Section 105)

Section 105 authorizes bilateral executive agreements permitting foreign governments to request data directly from US providers, bypassing traditional MLAT processes. Canada has been negotiating such an agreement since March 2022.[69]

The critical point for Canadian policymakers is structural. Section 103 establishes unilateral extraterritorial compulsion as the baseline. Section 105 does not constrain that power; it adds a parallel channel that normalizes direct access at surveillance scale, creating persistent, programmatic access to large volumes

of data without individualized judicial authorization. The policy question is therefore not whether an executive agreement creates new exposure, but whether Canada should consent to, accelerate and institutionalize a model that removes Canadian judicial gatekeeping from the evidentiary chain.[70]

While public data on Canadian MLAT processing times remains limited, capacity constraints should be addressed through resourcing and institutional reform rather than by displacing judicial mediation.

5.4 Why "Possession, Custody or Control" Defeats Data Residency Claims

A central vulnerability in Canadian approaches to cloud governance lies in the legal meaning of "possession, custody or control" under US law. The CLOUD Act deliberately shifts the jurisdictional trigger for compelled disclosure away from the physical location of data and toward the corporate and operational control exercised by service providers subject to US jurisdiction. This shift renders data residency — standing alone — an insufficient safeguard for Canadian data sovereignty.

US courts have long interpreted "possession, custody, or control" functionally rather than formally. The inquiry is not limited to where data are stored or which corporate entity nominally holds them, but whether the entity served with legal process has the *practical ability* to obtain the data. Courts routinely compel production where a parent corporation retains legal authority, technical access or operational leverage over data held by subsidiaries or affiliates, even where those entities are incorporated abroad and the data are stored extraterritorially.[71]

Recent scholarship analyzing the CLOUD Act confirms that the statute largely codifies this existing jurisprudence rather than creating a narrow or exceptional regime. Justin Hemmings, Sreenidhi Srinivasan and Peter Swire demonstrate that courts assess "control" along two principal axes: **legal control**, such as contractual rights, corporate governance authority or ownership interests; and **day-to-day operational control**, including routine administrative access, credentialed technical capability or centralized management of infrastructure.[72] Where either form of control is substantial, US courts have been prepared to compel production. Corporate separateness, internal access restrictions or localization architectures do not defeat jurisdiction where the parent entity can, in practice, cause the data to be produced.

This doctrine has direct implications for Canadian public-sector cloud procurement. Many arrangements marketed as "Canadian regions," "data residency solutions" or even "sovereign cloud" offerings preserve precisely the forms of control that US courts consider dispositive: centralized identity management, remote administrative access, unified security operations, parent-level audit rights, and contractual powers to reconfigure or access systems in exigent circumstances. In such configurations, data stored exclusively on Canadian soil may nonetheless fall squarely within the "possession, custody, or control" of a US-headquartered provider for purposes of US legal process.[73]

This implies a tiered approach to procurement. Providers should be assessed against sovereignty criteria including jurisdictional exposure, auditability and susceptibility to foreign compulsion. Trust is a legal condition, not a geopolitical presumption.

From a constitutional perspective, this exposure is not merely theoretical. **Canadian Charter jurisprudence has explicitly rejected the US "third-party doctrine,"** recognizing that individuals retain a reasonable expectation of privacy in digital records held by service providers.[74] This protection extends to Charter-protected persons whose data is subject to protection under section 8 of the Charter. The CLOUD Act, by contrast, operates within a US constitutional framework that treats provider-held data as subject to significantly weaker privacy protections. The result is a structural incompatibility: Canadian institutions may store data in cloud services in reliance on Canadian constitutional norms, while those same data remain legally accessible under a foreign constitutional order that Canada has deliberately declined to adopt.

Accordingly, assurances grounded in data localization, contractual commitments or voluntary corporate resistance to foreign orders cannot substitute for sovereign legal control. Where a cloud provider remains subject to US jurisdiction and retains operational or legal control over Canadian data, CLOUD Act exposure is a matter of legal architecture, not corporate intent. For Canadian policymakers, the relevant question is therefore not where data are stored, but who ultimately controls them, under which legal system and with what constitutional constraints.

5.5 Data Owner Rights and Protective Mechanisms: The Hard Limits

From the perspective of Canadian data subjects, the CLOUD Act provides no enforceable rights. Data owners are not notified of foreign demands, have no standing to challenge production orders and receive no post-disclosure remedy. Whatever procedural protections exist operate exclusively between the provider and the requesting state.[75]

Corporate contractual commitments and "sovereign cloud" assurances do not alter this reality. A provider subject to US jurisdiction cannot contract out of statutory disclosure obligations. When a valid US legal order is issued, compliance is mandatory, regardless of foreign law, customer agreements or data residency arrangements.[76]

5.5.1 Comity as a Limited and Discretionary Doctrine

Proponents of the CLOUD Act frequently invoke international comity as a safeguard against conflicts with foreign law. In theory, comity permits a US court to modify or quash an order where compliance would require a provider to violate the law of a foreign state. In practice, this protection is narrow, discretionary and structurally biased toward enforcement.

US courts have consistently treated comity not as a jurisdictional limitation but as a balancing exercise in which US investigative interests routinely prevail. The Bank of Nova Scotia cases illustrate the point: US courts enforced subpoenas against entities subject to US jurisdiction despite clear conflicts with foreign secrecy laws, imposing substantial fines for non-compliance.[77]

The CLOUD Act codifies rather than corrects this imbalance. Section 103(c) preserves comity only as an *ex post*, provider-initiated remedy. It confers no rights on affected data subjects, assigns no role to foreign courts, and provides no assurance that foreign constitutional standards will be respected.[78]

For Canadian purposes, comity is therefore not a meaningful safeguard. It does not restore Canadian judicial oversight, does not ensure Charter-equivalent protections and does not prevent unilateral execution of foreign legal process against Canadian-located data. It functions as a safety valve for providers — not as a sovereignty-preserving mechanism for states.[79]

6. MICROSOFT'S DIGITAL SOVEREIGNTY ASSURANCES: A CRITICAL ANALYSIS

6.1 Brad Smith's CLOUD Act Stance

In December 2025, Microsoft announced a landmark **C$19 billion investment in Canadian AI and cloud infrastructure** spanning 2023 to 2027, including more than C$7.5 billion over the next two years. This represents the most significant financial commitment in Microsoft Canada's history and is specifically directed toward building Canada's artificial intelligence capabilities and digital infrastructure.

The investment will expand Microsoft's Azure Canada Central and Canada East data centre regions, delivering secure, sustainable and scalable cloud and AI capabilities. New capacity is expected to come online in the second half of 2026.

President Brad Smith accompanied this announcement with pledges regarding Canadian digital sovereignty, including commitments to:

- Challenge US legal orders for access to Canadian customer data when they are overbroad, unlawful or conflict with Canadian law;
- Rely on comity-based arguments codified in the CLOUD Act to resist disclosure;
- Resist attempts — including executive orders — to cut off cloud services to Canadian government clients; and
- Leverage Microsoft's diplomatic relationships and pursue litigation where necessary.

6.2 The June 2025 French Senate Testimony

Any assessment of Microsoft's sovereignty assurances must be evaluated in light of the company's sworn testimony before the French Senate on June 10, 2025.[80]

When asked directly whether he could guarantee, under oath, that data of French citizens stored in Microsoft's cloud would never be transmitted to US authorities without explicit French authorization, Anton Carniaux, Microsoft France's Director of Public and Legal Affairs, responded unequivocally: "**Non, je ne peux pas le garantir** — "No, I cannot guarantee it."[81]

This admission, made under oath before a parliamentary body, confirms that Microsoft's corporate assurances — however well-intentioned — cannot override the company's legal obligations under US law. When a validly served US legal demand arrives, Microsoft must comply regardless of its contractual commitments to foreign customers.[82]

6.3 Why Microsoft's Assurances Are Insufficient for Canadian Sovereignty

From a sovereignty perspective, the fundamental question is whether Canadian institutions, not foreign legislatures or foreign courts, decide who may access sensitive Canadian data. Microsoft's commitments fail this test for several structural reasons.

6.3.1 Non-Sovereign Nature of Corporate Assurances

Microsoft's pledges represent a private actor's policy choice, subject to change at the company's discretion, rather than durable legal guarantees rooted in Canadian legislation, Canadian courts, or binding international agreements negotiated by Canada. Microsoft's admission "crystallizes a broader pattern of Canadian policy retreat in the digital domain" and demonstrates that "jurisdictional sovereignty in the age of cloud infrastructure defaults to the nation that controls the platform, not the country where the data resides."[83]

6.3.2 Legal Constraints Under US Law

The CLOUD Act explicitly authorizes US law enforcement to require US providers to disclose data they control, including data stored abroad. Microsoft, as a US corporation, remains ultimately subject to US law. The French Senate testimony confirmed what European regulators and privacy advocates have long suspected: technical and contractual measures cannot overcome legal obligations.

6.3.3 Limited Grounds for Challenge

The CLOUD Act provides only limited grounds, primarily comity, on which providers may challenge orders. Section 103(c) permits a provider to move to modify or quash an order if compliance would require violating the laws of a "qualifying foreign government." However, the seminal Bank of Nova Scotia cases from the 1980s demonstrate the severe limitations of comity-based challenges.[84]

In these cases, a US grand jury investigating drug trafficking and tax evasion subpoenaed records from the Bank of Nova Scotia's branches in the Bahamas and Cayman Islands. The bank argued that compliance would violate Bahamian bank secrecy laws and that principles of international comity should preclude enforcement. The Eleventh Circuit Court of Appeals rejected these arguments, holding that US courts would enforce subpoenas against entities subject to US jurisdiction even when compliance would violate foreign law. The court imposed substantial fines totaling US$1.825 million for non-compliance. The Supreme Court denied certiorari, leaving this aggressive precedent in place.

US courts have consistently applied the Restatement's comity balancing factors in a manner that prioritizes US governmental interests where a US entity has custody or control of documents.[85] As the Eleventh Circuit stated: "this court simply cannot acquiesce in the proposition that United States criminal investigations must be thwarted whenever there is conflict with the interest of other states."

6.4 Why Corporate Assurances Cannot Overcome Legal Obligations

The Bank of Nova Scotia precedent establishes the legal framework for evaluating all CLOUD Act challenges. US courts have consistently applied comity factors to prioritize US governmental interests when a US entity has custody or control of documents. The practical consequence is that corporate commitments to "challenge" or "resist" US legal demands, however well-intentioned, operate within a legal system that has repeatedly demonstrated its willingness to override foreign legal obligations when US interests are engaged.

This analysis does not suggest that corporate assurances are worthless. They may introduce procedural friction that delays compliance and provides opportunities for notice, but they cannot provide the legal protection that only Canadian law, applied by Canadian courts, can guarantee. (The policy implications are addressed in Section 12 below.)

7. COMPARATIVE CONSTITUTIONAL STANDARDS

7.1 The US Third-party Doctrine

Understanding the constitutional gulf between Canada and the United States on digital privacy requires examining the US "**third-party doctrine**," a constitutional principle that has no equivalent in Canadian jurisprudence.

The third-party doctrine originates from *Smith v Maryland* (1979).[86] The Supreme Court held that individuals have no "reasonable expectation of privacy" in information they voluntarily convey to third parties. Under this doctrine, the Fourth Amendment's protection against unreasonable searches does not apply to information held by banks, telephone companies, internet service providers or cloud storage companies.

7.2 Canadian Charter Protections: R. *v Spencer*

Canadian constitutional law has taken a fundamentally different path from the United States. In R. *v Spencer* (2014), the Supreme Court of Canada unanimously rejected the notion that privacy interests are extinguished when information is shared with third-party service providers.[87]

Justice Cromwell held that subscriber information "can reveal intimate details of the lifestyle and personal choices of the individual" and that "the Internet has become an extension of the individual's private existence." The Court explicitly rejected the American third-party doctrine, holding that "the reasonable expectation of privacy is a *normative* rather than a *descriptive* standard."

7.3 R *v Bykovets*: The "First Digital Breadcrumb"

The Supreme Court extended *Spencer*'s reasoning in R. *v Bykovets* (2024), holding that IP (internet protocol) addresses themselves are protected by Section 8 of the Charter.[88] Justice Karakatsanis described the IP address as "the first digital breadcrumb" that can reveal "a constellation of private information about the user."

7.4 The Constitutional Tension

The doctrinal divergence outlined above creates a fundamental problem for any Canada-US CLOUD Act agreement. Under the CLOUD Act framework, US authorities can obtain Canadian data from US-affiliated providers using legal standards that *Spencer* and *Bykovets* have declared unconstitutional in

Canada. The CLOUD Act does not require US authorities to satisfy Canadian constitutional standards before compelling disclosure of Canadian data — it requires only compliance with US law.

This is not a theoretical concern. As Citizen Lab has observed, "one would be hard pressed to find two democracies that are more incompatible when it comes to trying to align digital surveillance laws."[89] The incompatibility runs deeper than procedural differences: it reflects fundamentally different conceptions of the relationship between the individual, the state and the intermediaries that hold personal data.[90]

Cochranes analysis of CLOUD Act agreements under both Fourth Amendment and European Convention on Human Rights (ECHR) Article 8 frameworks demonstrates that the privacy safeguards embedded in existing agreements fall significantly short of the standards Canadians expect under the Charter.[91]

An executive agreement cannot resolve this tension — it can only paper over it by substituting US constitutional standards for Canadian ones whenever US authorities seek Canadian data.

8. CLOUD ACT EXECUTIVE AGREEMENTS

8.1 What a CLOUD Act "Executive Agreement" is

Under the US CLOUD Act, an "executive agreement" is a bilateral framework negotiated by the US Executive Branch that — once in force — permits foreign orders to be served directly on US service providers for data relating to serious crime, without routing the request through US courts via an MLAT for each request. In effect, it creates a standing authorization for provider-to-foreign-state disclosure under the foreign state's legal process, subject to the statutory conditions embedded in the CLOUD Act framework.

It is essential to understand what an executive agreement does and does not do. It does not create US authority to compel Canadian data — that authority already exists under Section 103 and is being exercised today. What an executive agreement does is provide reciprocal Canadian authority to demand data directly from US providers, formalize the bypass of MLAT processes for both parties and confer international law legitimacy on extraterritorial enforcement that currently operates unilaterally. For Canada, the trade-off is stark: marginal operational gains in exchange for surrendering the principle that foreign surveillance of Canadians requires Canadian institutional authorization.

8.1.1 Case Study: The UK-US CLOUD Act Agreement Shows the Operational Reality

The UK-US Executive Agreement (in force October 3, 2022; renewed in November 2024) provides the clearest evidence of how "direct access" operates once the machinery is built. The US Department of Justice's first-ever report to Congress on the Executive Agreement's implementation, submitted in November 2024, reveals the following:[92]

Volume and character of requests:

- As of October 2024, the United Kingdom issued **20,142 requests** to US service providers under the Executive Agreement.
- Over **99.8 percent** of these (20,105) were issued under the UK Investigatory Powers Act and were predominantly **wiretap/interception-style orders.**
- Fewer than **0.2 percent** (only 37 requests) were overseas production orders for stored communications data.

Comparative context: The United Kingdom's 20,142 wiretap-inclusive orders over two years dramatically exceeds US domestic practice. Federal and state law enforcement authorities in the United States (which has five times the population of the United Kingdom) obtained wiretap orders in criminal cases in only 4,507 instances during calendar years 2022 and 2023.[93]

US usage: The United States made only 63 requests to UK providers during the same period — a ratio of approximately 320:1.[94] The asymmetry reflects the concentration of major global service providers in the United States.

MLAT displacement failure: Contrary to the CLOUD Act's stated objective of alleviating MLAT burdens, the United Kingdom has continued using the MLAT process at the same rate as before the Executive Agreement.[95] Nearly all UK requests through the Executive Agreement could never have been made using MLATs, since MLATs cannot be used for real-time interception authority.

Provider concerns: The Department of Justice (DOJ) report noted that unnamed providers warned the DOJ about recent changes to UK law that could "impede changes to privacy and security features that U.S. providers offer globally."[96] This concern proved prescient when, in February 2025, the United Kingdom issued a Technical Capability Notice to Apple demanding global encryption backdoors.

8.2 Five Sovereignty-relevant Takeaways for Canada

1. **Direct access skews toward interception authorities.** The United Kingdom's overwhelming reliance on its interception statute demonstrates that executive agreements can become, in practice, high-volume channels for real-time surveillance — not merely stored "e-evidence" production.
2. **Stated congressional objectives are not being met.** The executive agreement has not reduced MLAT burdens or displaced traditional diplomatic channels.
3. **Secrecy constraints reduce visibility.** Provider nondisclosure obligations limit the ability to raise systemic concerns or conduct meaningful external scrutiny.
4. **Volume normalizes the bypass.** Once thousands of requests move outside MLAT processes, the exceptional becomes routine.
5. **Encryption attacks follow.** The United Kingdom leveraged its position under the Executive Agreement to demand global encryption backdoors, demonstrating how executive agreements can precede aggressive extraterritorial demands.

For Canada, the UK experience is an early warning that an executive agreement is not merely a faster MLAT. It is a different governance model: persistent direct access at surveillance scale.

8.3 Why an Executive Agreement Is Not Preferable for Canadian Digital Sovereignty

From a Canadian sovereignty standpoint, the objections to a CLOUD Act executive agreement are structural:

- **It replaces Canadian gatekeeping with corporate compliance.** Under MLAT, Canada's Central Authority and courts are the choke points. Under an executive agreement, the operational choke point becomes a provider's compliance team, subject to foreign law and secrecy obligations.
- **It shifts oversight away from Canadian constitutional standards.** Norms available to Canadian Charter Section 8 protected persons (reasonable expectation of privacy; rejection of the US third-party doctrine) do not apply to the request, the standard or the scope when the order is not executed through Canadian process.
- **It is designed to bypass the "foreign request to Canadian process" model.** That is the point of the instrument: speed via direct access. But "speed" here is achieved by removing a sovereignty layer, not by improving Canadian capacity.
- **It typically creates no enforceable rights for affected individuals.** Existing agreements disclaim the creation of individual rights or remedies, leaving data subjects with little recourse if data is accessed or misused.
- **It does not stop what is already happening.** Section 103 compulsion is operational now. An executive agreement would not reduce US access to Canadian data; it would add a second, normalized channel while removing the legal and diplomatic friction that currently attaches to unilateral extraterritorial demands.

Bottom line: an executive agreement is best understood as a direct-access architecture that treats cloud providers as cross-border enforcement intermediaries. That is governance by platform, not governance by Parliament.

8.3.1 Why "Efficiency" Is the Wrong Metric

Proponents of CLOUD Act executive agreements frequently frame the issue as one of operational efficiency, arguing that direct access to service providers is necessary to address delays associated with traditional MLAT processes. This framing is misleading and obscures the actual policy trade-off.

The delays associated with MLATs are not primarily legal or constitutional in nature. They are the result of capacity constraints, resourcing decisions and administrative under-investment, not an inherent inability of Canadian institutions to process foreign evidence requests. MLATs are deliberately designed to ensure that foreign investigative powers affecting Canadians are exercised through Canadian authorities, under Canadian law and subject to Canadian constitutional standards. As noted above, capacity constraints should be addressed through resourcing and institutional reform rather than by displacing Canadian judicial mediation.

Executive agreements do not "modernize" MLATs. They bypass them.

The speed gains achieved under an executive agreement are realized by removing Canadian judicial and governmental review, not by improving investigative cooperation. In practical terms, efficiency is purchased by eliminating the very safeguards that MLATs exist to preserve.

8.3.2 Canadian Officials Have Endorsed the CLOUD Act Model

A notable feature of the CLOUD Act debate is that Canadian public safety and justice officials have themselves articulated support for the framework, on grounds that inadvertently confirm the concerns this briefing raises.

Briefing materials from Public Safety Canada have characterized a potential CLOUD Act executive agreement with the United States as a mechanism to address "long delays in obtaining electronic evidence through traditional MLAT channels," emphasizing the need for "timely and effective" access to data for serious crime and cybercrime investigations.[97]

These statements are revealing not for what they advocate but for what they omit. The MLAT process is not slow because of a legal defect; it is slow because it routes foreign evidence demands through Canadian institutions, under Canadian law, subject to Canadian constitutional standards. The "delays" officials identify are the temporal cost of sovereignty. When Canadian authorities describe CLOUD Act agreements as enabling "timely and effective" access, they are describing the removal of Canadian judicial gatekeeping as a benefit, without acknowledging that this gatekeeping is what distinguishes lawful process from foreign surveillance.

8.4 The 2022 Announcement: Canada Enters CLOUD Act Negotiations

On March 22, 2022, at the re-established Canada-US Cross-Border Crime Forum in Washington, DC, Canada formally announced it had entered negotiations with the United States for a bilateral executive agreement under the CLOUD Act.[98] The announcement was made jointly by US Attorney General Merrick Garland and Secretary of Homeland Security Alejandro Mayorkas, together with Canada's then-Minister of Justice David Lametti and Minister of Public Safety Marco Mendicino.

The joint statement declared that the governments "welcomed negotiations for a potential bilateral agreement in relation to the U.S. Clarifying Lawful Overseas Use of Data Act (CLOUD Act)," stating that such an agreement "would allow Canadian and U.S. investigative authorities to, more efficiently and effectively, access communications and associated data in the other country when this information is needed for the prevention, detection, investigation, and prosecution of serious crime, such as terrorism, child sexual exploitation and abuse, and cybercrime, while respecting privacy and civil liberties."
These negotiations have proceeded without public discussion, disclosure or debate. Canadians have not been informed that their telecommunications metadata, banking records, insurance files and electronic

communications and associated electronic data, including both content and non-content information, are already subject to US legal process, nor have they been consulted on whether Canada should negotiate an agreement to facilitate such access.

8.5 Status of Negotiations: 2022–Present

As of December 2025, more than three years after the announcement, no Canada-US CLOUD Act agreement has been finalized.[99] The terms of the negotiations have not been made public, and the Canadian government has provided limited transparency regarding the status or substance of discussions.

As researchers Cynthia Khoo and Kate Robertson of The Citizen Lab observed in February 2025: "Since the 2024 U.S. Presidential election, Canada-U.S. relations have become increasingly strained and the subject of public concern. It should thus be of further concern to the public that, since 2022, the Canadian government has been quietly negotiating a bilateral law enforcement data-sharing agreement with the U.S. under the U.S. CLOUD Act. These negotiations are ongoing, even though the U.S. does not recognize human rights obligations beyond its own borders."[100]

8.6 Required Legislative Amendments

Implementation of a Canada-US CLOUD Act agreement would require substantial amendments to Canadian law. Canada would need to establish extraterritorial production orders, amend privacy legislation to authorize disclosures pursuant to foreign warrants and create reciprocal recognition mechanisms to give effect to US legal process in Canada.[101]

The Canadian Bar Association has recommended that any enabling legislation include a mechanism whereby foreign orders are reviewed by Canadian authorities for compliance with the bilateral agreement, and that Canadian service providers retain the right to seek review of requests in Canadian courts.[102]

8.7 Constitutional Concerns and Civil Society Opposition

Opposition to a Canada-US CLOUD Act agreement has intensified since negotiations were announced, uniting civil liberties organizations, privacy experts and the legal profession around a core concern: the constitutional incompatibility of Canadian and US surveillance law.

8.7.1 The Citizen Lab Analysis

In February 2025, researchers Khoo and Robertson of The Citizen Lab published a comprehensive analysis concluding that "one would be hard pressed to find two democracies that are more incompatible when it comes to trying to align digital surveillance laws." The analysis identified third-party doctrine

divergence, reproductive rights and civil liberties risks, and the "remedial no-man's land" created by existing CLOUD Act agreements, which "have explicitly refused to establish any rights or remedies for individuals or companies whose data is subject to seizure."

8.7.2 The Canadian Bar Associations

The Canadian Bar Association's (CBA's) Privacy and Access Law Section formally raised concerns about proceeding with a CLOUD Act agreement without substantial safeguards, submitting detailed recommendations in November 2024. The CBA's concerns included: preserving MLAT processes for requests targeting Canadians; exempting government data from CLOUD Act access; requiring Canadian judicial authorization before disclosure; amending privacy legislation to limit unintended disclosures; establishing notification requirements for Canadian data subjects; and creating mechanisms for Canadian judicial review of foreign orders.

8.7.3 Civil Liberties Coalition

In July 2025, the Canadian Civil Liberties Association (CCLA) joined 39 organizations and 122 experts in calling for withdrawal of Bill C-2, the Strong Borders Act, citing concerns that elements of the bill were "designed to align Canadian surveillance practices with U.S. practice, despite fundamental differences in our constitutional privacy protections and standards."[103]

8.8 CBA Recommendations for Canada-US CLOUD Negotiations

In November 2024, the CBA's Privacy and Access Law Section submitted detailed recommendations regarding any Canada-US CLOUD Act agreement:

1. Preserve MLAT for Canadians.
2. Exempt government data.
3. Amend the Criminal Code.
4. Clarify privacy laws.
5. Require Canadian notification.
6. Canadian judicial review.

The policy implications of this analysis, including the recommendation regarding the status of negotiations, are addressed in Section 12 below.

9. THE UK-APPLE ENCRYPTION CONTROVERSY: A WARNING FOR CANADA

9.1 The Technical Capability Notice

In February 2025, *The Washington Post* reported that the United Kingdom had secretly issued a Technical Capability Notice (TCN) to Apple under the Investigatory Powers Act 2016 (commonly known as the "Snoopers' Charter").[104] The order demanded that Apple create a backdoor allowing UK authorities to access *all* encrypted content uploaded to iCloud by *any* Apple user worldwide — not merely targeted accounts of UK residents.

This demand represents an extraordinary assertion of extraterritorial jurisdiction over encryption. The Investigatory Powers Act 2016 grants the UK Home Secretary authority to issue TCNs requiring telecommunications operators to maintain "permanent technical capabilities" enabling the interception of communications. Critically, the Investigatory Powers Act makes it a criminal offense for companies to disclose that they have received a TCN, creating a regime of secret compulsion.

Rather than comply, Apple chose to disable Advanced Data Protection for new UK users in February 2025. This decision meant that UK users lost access to the highest level of data protection available, but Apple avoided creating a global backdoor that would have compromised security for all users worldwide.

The legal asymmetry illustrated by the United Kingdom-United States example does not arise from any encryption-protective feature of the CLOUD Act itself, but from substantive limits embedded in US domestic law. US courts have *been reluctant* to compel the creation of encryption backdoors or new technical capabilities absent clear congressional authorization, including under the All Writs Act, reflecting concerns about undue burden and the limits of judicial authority in the absence of a statutory mandate.[105] The CLOUD Act preserves these domestic limits and is encryption-neutral rather than encryption-protective.[106]

By contrast, other jurisdictions, including the United Kingdom, maintain domestic legal authorities that permit the imposition of technical capability obligations. The constitutional concern is therefore not that the CLOUD Act mandates decryption, but that its executive agreement framework enables the cross-border circulation of data obtained under foreign legal regimes that permit surveillance powers incompatible with Canadian constitutional standards.

9.2 Cybersecurity Implications: The Salt Typhoon Warning

The catastrophic risks of building surveillance backdoors into communications infrastructure were dramatically illustrated by the Salt Typhoon cyberattacks disclosed in late 2024.[107] Salt Typhoon is an advanced persistent threat group attributed to China's Ministry of State Security. Beginning as early as 2022, Salt Typhoon infiltrated the networks of at least nine major US telecommunications companies, including AT&T, Verizon, T-Mobile and Lumen Technologies.

Most alarmingly, Salt Typhoon specifically targeted the systems used for **court-authorized wiretapping** — the very infrastructure mandated by the Communications Assistance for Law Enforcement Act to enable lawful intercept capabilities. Chinese intelligence operatives gained access to call detail records and, in some cases, the actual contents of communications. The US Federal Bureau of Investigation confirmed that the hackers specifically targeted individuals involved in government or political activity.

In January 2025, the US Treasury Department sanctioned Sichuan Juxinhe Network Technology Co., Ltd., a Chinese cybersecurity company identified as having direct involvement in Salt Typhoon operations.

The Salt Typhoon attacks validate what security researchers have long warned: **backdoors created for "lawful" surveillance will inevitably be discovered and exploited by malicious actors**. Any encryption backdoor demanded under a CLOUD Act agreement or domestic surveillance law creates a systemic vulnerability.

10. THE US POLICY CONTEXT: NATIONAL SECURITY STRATEGY AND DIGITAL DOMINANCE

Any assessment of CLOUD Act implications for Canada must be situated within the broader context of US digital policy. Recent developments make clear that the United States views technological dominance — including over cloud infrastructure, data flows and algorithmic systems — as a core national security priority.

10.1 The 2025 National Security Strategy

The November 2025 US National Security Strategy contains language with direct implications for Canadian digital sovereignty. The Strategy's Western Hemisphere section declares that "the terms of our agreements, especially with those countries that depend on us most and therefore over which we have the most leverage, must be sole-source contracts for our companies" and states that Washington should "make every effort to push out foreign companies that build infrastructure in the region."[108]

The Strategy instructs every US embassy to identify commercial opportunities for American firms and directs all US officials to serve as commercial advocates. It emphasizes "U.S.-built energy infrastructure, U.S.-backed access to critical minerals, and cyber networks secured with American technology."[109] These formulations suggest that allied markets may be viewed as captive rather than competitive.

10.2 The White House AI Action Plan

The July 2025 White House AI Action Plan declares it a "national security imperative for the United States to achieve and maintain unquestioned and unchallenged global technological dominance."[110] The Plan fuses AI development with "financial infrastructure, cloud dominance, and payment systems,"[111] positioning algorithmic power as a national asset. This framing has direct implications for how CLOUD Act powers may be deployed and expanded.

10.3 The USMCA Review and Digital Governance

The ongoing 2025 United States-Mexico-Canada Agreement (USMCA) Review provides further context. US Trade Representative Jamieson Greer's December 10, 2025 remarks at the Atlantic Council confirmed that the United States is conducting the review through bilateral rather than trilateral channels and described it as a "forcing function" that could lead to "a replacement" of the agreement.[112] Ambassador Greer acknowledged using tariff negotiations to pressure digital governance outcomes, noting disappointment that the European Union has shown "zero moderation" in digital enforcement and reaffirming that the United States will not "allow that regulation to be outsourced."

These developments suggest that trade tools are increasingly being deployed to influence digital governance outcomes, heightening the risk that CLOUD Act mechanisms may be leveraged as part of broader economic pressure campaigns.

10.4 Implications for Canadian Policy

As this author argued in his December 2025 rebuttal testimony to the US Trade Representative, Canadian digital sovereignty is not a threat to US interests but a strategic asset for both countries.[113] A Canada that retains the legal and institutional capacity to exclude high-risk providers, audit AI systems and enforce its own cybersecurity standards provides "trusted capacity within the hemisphere" and "regulatory diversity rather than technological monoculture."[114] The USMCA review should "codify, not pre-empt" democratically determined digital sovereignty arrangements.

10.5 Trade and Treaty Considerations

Concerns are sometimes raised that Canadian measures to protect digital sovereignty, such as sovereign cloud procurement criteria, jurisdictional exclusions, or encryption key controls, could conflict with Canada's trade obligations, particularly under the Canada-United States-Mexico Agreement (CUSMA) or USMCA.

These concerns are addressed in detail in Section 12 of this report, which analyzes how the seven-pillar framework for Canadian response can be implemented consistently with Canada's trade commitments. The short answer is that CUSMA contains explicit national security, law enforcement and public policy exceptions that preserve Canada's authority to regulate in areas implicating constitutional rights, public safety and the administration of justice. Jurisdiction-based procurement criteria that focus on control, auditability and encryption-key custody are governance measures, not prohibited data localization requirements.

Trade agreements are not suicide pacts. They do not require Canada to surrender constitutional control over its data.

11. THE CLOUD ACT IN THE LONGER U.S. PATTERN OF EXTRATERRITORIAL REACH

The CLOUD Act is not an anomaly. It is the data-access counterpart to a longer US practice of asserting extraterritorial jurisdiction where US interests are engaged, shifting jurisdictional hooks away from territory and toward **nexus** (corporate presence, control, financial rails, infrastructure dependence). The CLOUD Act's key move is to make **provider "possession, custody or control"** — not server location — the trigger for compelled disclosure, anchoring extraterritorial reach in corporate structure and operational access.

11.1 How Canada has Responded in the Past: FEMA as a Sovereignty Template

Canada has not been passive in the face of US extraterritorial measures. The principal domestic tool is the ***Foreign Extraterritorial Measures Act (FEMA)***, which empowers cabinet/Attorney General mechanisms to restrict compliance with foreign measures that adversely affect Canadian interests. FEMA has been used as a sovereignty shield, including by blocking orders in response to US extraterritorial sanctions and procurement measures.

11.2 FEMA's Potential Application to Digital Data Compulsion

FEMA's existing architecture, while developed primarily in response to US economic sanctions against Cuba, contains provisions that could be adapted to address the CLOUD Act's compulsion to obtain Canadian data. Section 3 of FEMA permits the Attorney General to issue orders prohibiting or restricting the production and disclosure to a foreign tribunal of documents located in Canada or under the possession or control of Canadian citizens or residents, and the giving of evidence by Canadian citizens or residents to foreign tribunals.[115]

These powers may be exercised when the Attorney General is of the opinion that the foreign tribunal is exercising powers that "adversely affect significant Canadian interests in relation to international trade or commerce involving a business carried on in whole or in part in Canada" or that "infringe Canadian sovereignty."[116]

11.3 Adaptation Challenges

Several challenges would need to be addressed before FEMA could serve as an effective blocking mechanism for CLOUD Act demands:

1. **Definition of "foreign tribunal"**: CLOUD Act demands are served directly on providers by US law enforcement agencies, typically without judicial involvement at the demand stage. Whether an

agency subpoena or National Security Letter qualifies as action by a foreign tribunal under FEMA remains unclear.

2. **Conflict of laws for dual-listed companies**: Canadian telecommunications providers with US stock exchange listings (BCE, Rogers, TELUS) face structural conflicts: FEMA compliance could jeopardize their US market access and Security Exchange Commission reporting obligations, while CLOUD Act compliance could violate FEMA.[117]
3. **Enforcement practicality**: FEMA violations require prosecution with consent of the Attorney General of Canada.[118] There have been no prosecutions under the existing Cuba-related FEMA Order, despite apparent violations.
4. **Provider-side enforcement cap**: FEMA orders bind Canadian persons and corporations, but the ultimate target of CLOUD Act compulsion, the US-headquartered cloud provider, is beyond Canadian jurisdictional reach.

11.4 The Legal Effect of FEMA Blocking Orders

It is important to understand what FEMA can and cannot accomplish. FEMA cannot compel US-headquartered providers to refuse CLOUD Act demands; those providers are subject to US jurisdiction and US law. What FEMA can do is create a legal conflict that strengthens comity-based challenges in US courts, impose compliance obligations on Canadian subsidiaries and affiliates of US providers, and establish procurement conditions that favour providers not subject to conflicting foreign legal obligations.

The 2014 FEMA Order regarding the Alaska "Buy America" ferry terminal project demonstrates that Canada can and will use FEMA in specific commercial contexts.[119] Whether there is political will to extend this model to digital infrastructure is a policy question, not a legal one.

Specific recommendations for FEMA modernization, including proposed legislative amendments, are set out in Section 12, Pillar B.

11.5 What Canada Can Do Now: A Framework for Response

Opposition to a Canada-US CLOUD Act agreement has intensified since negotiations were announced, uniting civil liberties organizations, privacy experts and the legal profession around a core concern: the constitutional incompatibility of Canadian and US surveillance law.

11.5.1 Immediate Executive Actions (No Legislative Change Required)

The federal government can act immediately on several fronts: suspending CLOUD Act executive agreement negotiations pending constitutional assessment; auditing government cloud deployments for CLOUD Act exposure; issuing procurement guidance requiring sovereignty impact assessments; and commissioning independent legal analysis of existing US-UK and US-Australia agreements.

11.5.2 Legislative Modernization

FEMA provides a foundation for blocking legislation but requires amendment to address digital data compulsion effectively. Parliament can expand FEMAs scope to cover CLOUD Act demands, create sector-specific blocking orders, establish mandatory disclosure requirements and introduce civil penalties with automatic stay mechanisms.

11.5.3 Technical and Institutional Investment

Longer-term measures include migrating critical infrastructure to Canadian-controlled systems, mandating customer-controlled encryption for sensitive government data, investing in MLAT processing capacity and establishing disclosure obligations for critical infrastructure providers.

Section 12 below provides detailed recommendations organized by policy domain, with specific actions, responsible authorities and implementation timelines.

12. POLICY RECOMMENDATIONS: A SEVEN-PILLAR FRAMEWORK

The following recommendations are organized by policy domain and implementation timeframe. Each is designed to be actionable within existing constitutional authority. Together, they constitute a comprehensive response to the sovereignty challenges posed by the CLOUD Act.

12.1 CLOUD Act Negotiations: Suspend and Reassess

Central recommendation: Canada should suspend CLOUD Act executive agreement negotiations with the United States until constitutional compatibility concerns are resolved and robust safeguards — exceeding those in existing US-UK and US-Australia agreements — can be guaranteed.

12.1.1 Rationale

Since March 2022, Canada has been negotiating a bilateral executive agreement under Section 105 of the CLOUD Act. What Canadians must understand is that Section 103 — authorizing unilateral extraterritorial compulsion — is already operational. US authorities can today demand Canadian data from any provider subject to US jurisdiction, without notification to affected Canadians and without Canadian judicial review. An executive agreement would not create this exposure; it would formalize and accelerate it while removing the MLAT's sovereignty layer entirely.

The existing US-UK agreement demonstrates operational reality at persistent, programmatic access to large volumes of data without individualized judicial authorization — what I call surveillance scale: the United Kingdom issued over 20,000 requests to US providers in two years, overwhelmingly for real-time interception rather than stored data.[120] As The Citizen Lab concluded: "One would be hard pressed to find two democracies that are more incompatible when it comes to trying to align digital surveillance laws."[121]

Specific actions:

1. **Formally suspend negotiations** pending completion of a comprehensive constitutional impact assessment examining compatibility with *Spencer*, *Bykovets* and Section 8 of the Charter.
2. **Commission an independent legal analysis** comparing existing CLOUD Act agreements (United States-United Kingdom, United States-Australia) with Canadian constitutional standards, to be made public before any executive agreement is finalized.
3. **Require parliamentary review** of any proposed agreement through the Standing Committee on Public Safety and National Security, the Standing Committee on Science and Research, and the Standing Committee on Justice and Human Rights before ratification.
4. **Establish non-negotiable conditions** for any future agreement, including: preservation of Canadian judicial authorization before Canadian data can be disclosed to US authorities; notification

requirements for Canadian data subjects; enforceable remedies for individuals whose data is improperly accessed; and explicit carve-outs for government data and critical infrastructure.

12.2 Legislative Reform: Modernize Canada's Blocking Legislation

Central recommendation: amend FEMA to address digital data compulsion and create meaningful legal consequences for unauthorized disclosure of Canadian data to foreign authorities.

12.2.1 Rationale

FEMA provides the Attorney General with the authority to prohibit compliance with foreign measures that adversely affect Canadian interests or infringe Canadian sovereignty.[122] However, FEMA was developed primarily in response to US economic sanctions against Cuba and requires adaptation for the digital context. Several challenges must be addressed: the definition of "foreign tribunal" may not clearly encompass direct agency demands under the CLOUD Act; dual-listed Canadian companies face structural conflicts between FEMA compliance and US regulatory obligations; and enforcement mechanisms lack practical deterrent effect.

Specific legislative amendments:

1. **Expand FEMA's scope** to expressly cover disclosure demands under foreign data access laws, including the CLOUD Act, National Security Letters and equivalent instruments.
2. **Create sector-specific blocking orders** for telecommunications providers, financial institutions and critical infrastructure operators, establishing clear obligations and consequences.
3. **Establish mandatory disclosure requirements** requiring Canadian entities to notify designated Canadian authorities when they receive foreign compulsion demands affecting Canadian data.
4. **Introduce civil penalties and automatic stay mechanisms** that create genuine compliance friction, moving beyond the current regime where violations require prosecution with Attorney General consent.
5. **Create statutory safe harbour** for Canadian entities that refuse to comply with foreign data demands in reliance on FEMA blocking orders, protecting them from contractual and regulatory consequences.

Note on effectiveness: FEMA blocking orders cannot directly compel US-headquartered providers to resist US legal process. However, they can: create legal conflict that strengthens comity-based challenges under 18 U.S.C. § 2703(h); impose obligations on Canadian subsidiaries and affiliates; establish conditions for government procurement; and signal sovereign intent in international negotiations.[123]

12.3 Critical Infrastructure: Migrate to Canadian-controlled Systems

Central recommendation: migrate critical government systems — particularly national defence and security operations, government continuity, and income support and pensions —to Canadian-controlled infrastructure not subject to US jurisdiction under the CLOUD Act.

12.3.1 Rationale

Over 80 percent of Canadian cloud services rely on foreign infrastructure.[124] The DND and CAF make significant use of Microsoft 365 through Defence 365, which serves as a common cloud infrastructure for collaboration across the DND/CAF. Under current arrangements, any data on these systems could, in theory, be subpoenaed by US authorities without Canadian judicial review. As the Privacy Commissioner noted: "data residency requirements alone cannot guarantee protection from foreign legal processes."[125]

Microsoft's June 2025 testimony before the French Senate confirmed this vulnerability with devastating clarity, as previously noted. When asked whether he could guarantee French government data would not be transmitted to US authorities without French authorization, Microsoft France's Carniaux responded that he could not provide such a guarantee. The same is true for Canadian data.

Specific actions:

1. **Conduct an immediate audit** of all federal government cloud deployments to identify systems storing classified, protected or sensitive information on infrastructure subject to CLOUD Act jurisdiction.
2. **Establish migration timeline** for Defence 365 and equivalent national security systems to Canadian-controlled alternatives, with interim technical protections (customer-controlled encryption) during transition.
3. **Invest in Canadian cloud capacity** through public-private partnerships or direct investment in Shared Services Canada infrastructure, ensuring availability of sovereign alternatives for government workloads.
4. **Define "sovereign cloud" in procurement policy** based on four criteria: jurisdictional control (provider not subject to foreign compulsion laws); operational control (Canadian administration without foreign override); cryptographic control (customer or Canadian authority holds encryption keys); and audit and enforcement authority (Canadian institutions possess meaningful oversight).

12.4 Procurement Reform: Sovereignty-based Criteria

Central recommendation: revise federal procurement policy to require sovereignty impact assessments for cloud services and establish mandatory criteria for sensitive government data.

12.4.1 Rationale

Current procurement frameworks treat cloud services primarily as commodity IT (internet technology) purchases rather than sovereignty-implicating infrastructure decisions. The result is that jurisdictional exposure to foreign legal process is not systematically assessed, and "data residency" requirements are treated as sufficient protection when they manifestly are not.

Specific actions:

1. **Amend the Treasury Board Directive on Service and Digital** to require sovereignty impact assessments for all cloud procurements involving protected or classified information.
2. **Establish tiered procurement requirements** based on data sensitivity: Tier 1 (classified/national security) — Canadian-controlled providers only, customer-held encryption keys mandatory; Tier 2 (protected/sensitive) — sovereignty-compliant providers preferred, encryption required; and Tier 3 (unclassified) — standard procurement with disclosure of jurisdictional exposure.
3. **Require provider disclosure** of corporate structure, US jurisdictional exposure (stock listings, subsidiaries, US customers) and compliance history with foreign legal process.
4. **Include contractual termination rights** triggered by provider compliance with foreign data demands affecting Canadian government data without Canadian authorization.

12.5 Technical Protections: Mandate Encryption Standards

Central recommendation: Mandate customer-controlled encryption for sensitive government data, ensuring that providers cannot comply with foreign disclosure demands because they cannot access intelligible data.

12.5.1 Rationale

Technical protections succeed where legal assurances fail. A provider cannot disclose data it cannot access. Customer-controlled encryption (where the government customer, not the cloud provider, holds decryption keys) creates a technical barrier to foreign compulsion that operates regardless of the provider's legal obligations. The UK-Apple encryption controversy demonstrates both the importance of encryption and the pressure providers face to compromise it.[126]

Specific actions:

1. **Require customer-managed encryption keys** for all Tier 1 and Tier 2 government cloud deployments, with keys held by Canadian government authorities rather than providers.

2. **Establish key management infrastructure** within Shared Services Canada or the Communications Security Establishment Canada to support government-wide encryption key custody.
3. **Prohibit acceptance of encryption backdoor demands** by providers serving Canadian government clients, with contractual consequences for compliance with foreign demands to weaken encryption.
4. **Develop Canadian cryptographic standards** for government cloud deployments through the Canadian Centre for Cyber Security, ensuring interoperability while maintaining sovereign control.

12.6 Institutional Capacity: Invest in MLAT Infrastructure

Central recommendation: address MLAT delays through capacity investment rather than sovereignty bypass, preserving Canadian judicial oversight while improving operational efficiency.

12.6.1 Rationale

Proponents of CLOUD Act executive agreements frequently frame the issue as one of operational efficiency, arguing that direct provider access is necessary to address MLAT delays. This framing is misleading. The delays associated with MLATs are not primarily legal or constitutional in nature — they result from capacity constraints, resourcing decisions and administrative underinvestment. MLATs are deliberately designed to ensure that foreign investigative powers affecting Canadians are exercised through Canadian authorities, under Canadian law and subject to Canadian constitutional standards. Executive agreements do not "modernize" MLATs; they bypass them.

Specific actions:

1. **Increase staffing and technical capacity** within Canada's MLAT central authority (International Assistance Group, Department of Justice) to reduce processing times.
2. **Establish service-level standards** with treaty partners, committing to specified response times for priority categories of requests.
3. **Digitize and standardize request formats** to reduce administrative burden and enable faster processing.
4. **Prioritize serious-crime requests** through existing judicial channels, ensuring that legitimate law enforcement needs are met without abandoning constitutional oversight.
5. **Publish annual statistics** on MLAT request volumes, processing times and outcomes to enable evidence-based assessment of capacity needs.

12.7 Private Sector Obligations: Transparency and Compliance Framework

Central recommendation: establish disclosure obligations for Canadian telecommunications and critical infrastructure providers regarding CLOUD Act exposure, enabling informed decisions by consumers, businesses and government procurement officers.

12.7.1 Rationale

Major Canadian telecommunications providers (BCE, Rogers, TELUS) and technology companies (Shopify) maintain US connections — stock exchange listings, subsidiaries, institutional investors — that may expose them to CLOUD Act jurisdiction. Canadians cannot make informed choices about their data if this exposure is not disclosed.

Specific actions:

- **Require annual disclosure** by designated critical infrastructure providers of: corporate structure and foreign jurisdictional exposure; volume of foreign legal demands received; volume of demands complied with; and categories of data affected.
- **Establish notification requirements** obligating providers to inform Canadian customers when their data has been disclosed to foreign authorities, subject to limited exceptions for ongoing investigations.
- **Create regulatory guidance** through the Canadian Radio-television and Telecommunications Commission and the Office of the Superintendent of Financial Institutions on CLOUD Act risk assessment and mitigation for regulated entities.
- **Consider designation authority** enabling the Minister of Innovation, Science and Industry to designate specific providers as "critical digital infrastructure" subject to enhanced oversight and national security review of foreign acquisitions.

13. CONCLUSION

Canada faces a defining choice on digital sovereignty. The question is not whether the CLOUD Act poses risks to Canadian data. That question has been answered. Microsoft's June 2025 testimony before the French Senate removed any remaining doubt: US-headquartered providers cannot guarantee that Canadian data will remain beyond the reach of US legal process, regardless of where that data is stored or what contractual commitments are made.

The question now is what Canada will do about it.

Three realities should guide Canadian policy. First, the status quo is untenable. Over 80 percent of Canadian cloud services depend on foreign infrastructure. Critical government systems operate on platforms subject to CLOUD Act jurisdiction. This is not a theoretical vulnerability; it is an operational fact. Second, the legal protections Canada might rely upon provide less security than official statements suggest. The Bank of Nova Scotia precedent confirms that US courts will enforce disclosure orders even when compliance requires violating foreign law. The UK experience confirms these concerns at operational scale. Third, the bilateral context has shifted. The November 2025 US National Security Strategy characterizes allied markets as opportunities for American commercial dominance. Canada should calibrate its expectations accordingly.

Section 12 above sets out a comprehensive seven-pillar framework for a Canadian response. The recommendations address the full spectrum of available measures, from immediate executive actions requiring no legislative change to longer-term institutional reforms. Together, they constitute a coherent strategy for preserving Canadian sovereignty over Canadian data.

The Supreme Court of Canada has articulated a constitutional vision in which Canadians retain a reasonable expectation of privacy in their electronic communications, even when those communications are held by third-party service providers. The CLOUD Act operates within a constitutional framework that reaches the opposite conclusion. These two visions cannot be reconciled through corporate goodwill or contractual drafting.

Canada must choose which constitutional order will govern Canadian data.

The decisions made in the coming months will shape Canada's digital sovereignty for a generation. They deserve the attention this briefing has sought to provide.

The policy window is open. CLOUD Act negotiations remain incomplete. Critical infrastructure and procurement decisions are being made. The USMCA review creates both risks and opportunities for digital governance. In each of these domains, Canada retains agency, but only if it exercises that agency deliberately.

14. APPENDIX: RECOMMENDED READING LIST

The following sources provide essential background for understanding the CLOUD Act and Canadian digital sovereignty.

14.1 Official US Government Documents

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.

The White House, "AI Action Plan," (23 July 2025).

US Department of Justice, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act," (April 2019), https://www.justice.gov/opa/press-release/file/1153446/download.

14.2 USMCA Review Materials

Appleton, Barry, "Law, Not Leverage: A Rules-Based Path for the USMCA Review — Rebuttal Comments to the US Trade Representative," Docket No. USTR-2025-0004 (December 12, 2025), https://ssrn.com/abstract=5668791.

Atlantic Council, "Inside the Trump trade strategy with US Trade Representative Jamieson Greer," Transcript (December 10, 2025), https://www.atlanticcouncil.org/news/transcripts/inside-the-trump-trade-strategy-with-us-trade-representative-jamieson-greer.

14.3 U.S. Personal Jurisdiction and Digital Services

The following sources provide authoritative analysis of how US courts assess personal jurisdiction over foreign defendants in cases involving online services, digital platforms and cross-border commercial activity. These materials reflect US doctrine and are relied upon by courts, practitioners and government agencies, including in contexts relevant to CLOUD Act exposure.

Borchers, Patrick J., "Jurisdictional Pragmatism: International Shoe's Half-Buried Legacy," 28 *UC Davis Law Review* 561 (1995).

Freer, Richard D., "Personal Jurisdiction in the Twenty-First Century: The Ironic Legacy of International Shoe," 63 *South Carolina Law Review* 551 (2012).

Robertson, Cassandra Burke, "Personal Jurisdiction in the Internet Age," 38 *Tulsa Law Review* 299 (2003).

Sachs, Stephen E., "How Congress Should Fix Personal Jurisdiction," 108 *Harvard Law Review* 1301 (2019).

Stein, Allan R., "Personal Jurisdiction and the Internet: Seeing Due Process Through the Lens of Regulatory Precision," 98 *Northwestern University Law Review* 411 (2004).

14.4 Official US Government Interpretations of the CLOUD Act

US Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (April 2019).

U.S. Department of Justice, *Report to Congress on the Implementation of the U.S.-U.K. CLOUD Act Agreement* (2023).

14.5 Legal Commentary and Analysis

Appleton, Barry, "The Cloud Casts a Long Shadow: Microsoft, the CLOUD Act, and Canada's Vanishing Digital Sovereignty" Appleton's Clause & Effect (21 July 2025), online: https://barryappleton.substack.com/p/the-cloud-casts-a-long-shadow.

Appleton, Barry, "Canada is ceding sovereignty to America's 'algorithmic empire'" National Post (15 September 2025), online: https://nationalpost.com/opinion/canada-is-ceding-sovereignty-to-americas-algorithmic-empire.

Appleton, Barry, "Canada surrenders to foreign code," National Post (October 15, 2025), https://nationalpost.com/opinion/canada-surrenders-to-foreign-code.

BSA | The Software Alliance, "The US CLOUD Act: Myths vs. Facts," (April 2019), https://www.bsa.org/files/policy-filings/04112019uscloudactmyth.pdf.

Canadian Bar Association, Privacy and Access Law Section, "Submission on CLOUD Act Agreement," (November 2024), https://nationalmagazine.ca/en-ca/articles/cba-influence/submissions/2025/how-to-address-canada-s-digital-data-disclosures-with-the-u-s.

Daskal, Jennifer, "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0," (2019) 71:9 *Stanford Law Review* 9.

Mulligan, Stephen P., *Cross-Border Data Sharing Under the CLOUD Act*, Congressional Research Service Report R45173 (updated periodically).

The Citizen Lab, "Canada-U.S. Cross-Border Surveillance Negotiations Raise Constitutional and Human Rights Concerns," (February 2025).

14.6 Official Canadian Government Documents

Treasury Board of Canada Secretariat, "Direction on Electronic Data Residency," (August 2025).

Privacy Commissioner of Canada, Annual Report to Parliament 2023-24, (Office of the Privacy Commissioner, 2024).

Office of the Information and Privacy Commissioner for British Columbia, "Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing," (October 2004), https://www.oipc.bc.ca/special-reports/1271.

14.7 Key US Statutes

Clarifying Lawful Overseas Use of Data Act, Pub L No 115-141, Div V (2018), codified at 18 USC § 2713.

Stored Communications Act, 18 USC §§ 2701-2713.

Electronic Communications Privacy Act of 1986, Pub L No 99-508, 100 Stat 1848.

14.8 Key Canadian Statutes

Foreign Extraterritorial Measures Act, RSC 1985, c F-29.

Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165.

14.9 Key US Cases

In *Re Grand Jury Proceedings (Bank of Nova Scotia)*, 691 F 2d 1384 (11th Cir 1982); 740 F 2d 817 (11th Cir 1984).

International Shoe Co v Washington, 326 US 310 (1945).

Smith v Maryland, 442 US 735 (1979).

Société Nationale Industrielle Aérospatiale v United States District Court, 482 US 522 (1987).

14.10 Key Canadian Cases

R v Bykovets, 2024 SCC 6.

R v Love, 2022 ABCA 269.

R v Spencer, 2014 SCC 43, [2014] 2 SCR 212.

14.11 News and Investigative Reporting

French Senate, "Commande publique : audition de Microsoft," (June 10, 2025), https://www.senat.fr/actualite/commande-publique-audition-de-microsoft-5344.html.

Menn, Joseph, "U.K. orders Apple to let it spy on users' encrypted accounts," *The Washington Post* (February 7, 2025).

Rudolph, Alexander, "Microsoft Admits: US Law Supersedes Canadian Sovereignty," Canadian Cyber in Context (July 21, 2025), https://www.cyberincontext.ca/p/microsoft-admits-us-law-supersedes.

14.12 DOJ Reports and Congressional Materials

Nojeim, Greg, "CLOUD Act, Encryption, and Americans' Privacy," Written Testimony before the House Judiciary Committee, Subcommittee on Crime and Federal Government Surveillance (June 5, 2025), https://www.congress.gov/119/meeting/house/118335/witnesses/HHRG-119-JU08-Wstate-NojeimG-20250605.pdf.

US Department of Justice, *Report to Congress on the Implementation of the U.S-U.K. CLOUD Act Agreement*, (November 2024), https://www.documentcloud.org/documents/25551978-doj-report-to-congress-on-us-uk-cloud-act-agreement.

14.13 Commentary on Implementation

Center for Democracy and Technology, "Secrets, Secrets Are No Fun: the United Kingdom's Secret War on Encryption," (March 25, 2025), https://cdt.org/insights/secrets-secrets-are-no-fun-the-united-kingdoms-secret-war-on-encryption/

Gidari, Albert, "The Big Interception Flaw in the US-UK Cloud Act Agreement," *Stanford Law School Center for Internet and Society*, (October 2019), https://cyberlaw.stanford.edu/blog/2019/10/big-interception-flaw-us-uk-cloud-act-agreement.

Salgado, Richard, "First Insights Into the U.S.-U.K. CLOUD Act Agreement," *Lawfare*, (March 10, 2025), https://www.lawfaremedia.org/article/first-insights-into-the-u.s.-u.k.-cloud-act-agreement.

Shurson, Jessica, "Assessing the US-UK CLOUD Act Agreement" *Issues in Cybercrime Law*, (March 13, 2025), https://issuesincybercrimelaw.substack.com/p/assessing-the-us-uk-cloud-act-agreement.

14.14 Canadian Civil Society

Canadian Civil Liberties Association, "Bill C-2 Explainer: Information-sharing between Canada & the US," (October 2025), https://ccla.org/wp-content/uploads/2025/10/Bill.C-2.Explainer-Canada.US_.information.sharing.pdf.

END NOTES

[1] Cynthia Khoo and Kate Robertson, "Canada-U.S. Cross-Border Surveillance Negotiations Raise Constitutional and Human Rights Whirlwind Under U.S. CLOUD Act," (The Citizen Lab, February 24, 2025) https://citizenlab.ca/2025/02/canada-us-cross-border-surveillance-cloud-act.

[2] The White House, National Security Strategy of the United States of America (November 2025) at 18-19, https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.

[3] The White House, AI Action Plan (July 23, 2025).

[4] *Clarifying Lawful Overseas Use of Data Act*, HR 4943, 115th Cong, Pub L No 115-141, Div V (2018), codified at 18 USC § 2713 (herein referred to as the "CLOUD Act"); US DOJ, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act" (April 2019), https://www.justice.gov/d9/press-releases/attachments/2019/04/10/department_of_justice_cloud_act_white_paper_2019_04_10_final_0.pdf.

[5] *Stored Communications Act*, Pub. L. No. 99-508, tit. II, 100 Stat. 1848 (1986), codified as amended at 18 USC § 2701–2713. The Act was amended by the CLOUD Act in 2018 to clarify that disclosure obligations apply to data within a provider's "possession, custody, or control," regardless of storage location.

[6] Treasury Board of Canada Secretariat, "Government of Canada White Paper: Data Sovereignty and Public Cloud" (2018, updated 2023), https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/gc-white-paper-data-sovereignty-public-cloud.html (stating that "[a]s long as a CSP that operates in Canada is subject to the laws of a foreign country, Canada will not have full sovereignty over its data"); IDC Canada, Canadian Cloud Services Market Analysis (2024) (reporting that over 80 percent of Canadian enterprises use foreign-headquartered cloud providers); Cybersecure Policy Exchange (Dais), Toronto Metropolitan University, Submission on Canada's National Cyber Security Strategy (June 2024), https://dais.ca/reports/submission-for-canadas-national-cyber-security-strategy (identifying foreign cloud dependency as a significant national security concern).

[7] Alexander Rudolph, "Microsoft Admits: US Law Supersedes Canadian Sovereignty," Canadian Cyber in Context, July 21, 2025, https://www.cyberincontext.ca/p/microsoft-admits-us-law-supersedes.

[8] Privacy Commissioner of Canada, Annual Report to Parliament 2023-24 (Ottawa: Office of the Privacy Commissioner, 2024) at 34.

[9] See *Gucci America, Inc. v Weixing Li*, 768 F.3d 122 (2d Cir. 2014); *In re Vitamin C Antitrust Litigation*, 837 F.3d 175 (2d Cir. 2016). US courts apply a functional test examining whether the entity served with process has the practical ability to obtain the documents, regardless of formal corporate separateness.

[10] *International Shoe Co. v Washington*, 326 US 310, 316 (1945). For analysis of how personal jurisdiction doctrine applies in the CLOUD Act context, see Tim Cochrane, "Hiding in the Eye of the Storm Cloud: How CLOUD Act Agreements Expand U.S. Extraterritorial Investigatory Powers," *Duke Journal of Comparative & International Law* 32, no. 1 (2021): 153, 187–201.

[11] Andrew Clement, "IXmaps: Tracking Your Personal Data Through the NSA's Warrantless Wiretapping Sites," *Proceedings of the IEEE International Symposium on Technology and Society* (2014); IXmaps Research Project, *Canadian Internet Routing and NSA Surveillance Vulnerabilities*, University of Toronto Faculty of Information, https://ixmaps.ca. Clement's multi-year research project documented that substantial volumes of domestic Canadian internet traffic transit through US network exchange points — including facilities identified as National Security Agency surveillance nodes — before returning to Canadian recipients, thereby exposing nominally Canadian communications to US interception authority.

[12] Barry Appleton, "Railway of the Future: Ottawa Is Letting Foreign Countries Dictate Our Governance," *National Post*, September 30, 2025, A9, https://nationalpost.com/opinion/ai-and-cloud-infrastructure-is-the-railway-of-the-future-why-isnt-canada-building-it; EPFL, ETH Zurich and Swiss National Supercomputing Centre (CSCS), "Apertus: A Fully Open, Transparent, Multilingual Language Model," press release, September 2, 2025, https://actu.epfl.ch/news/apertus-a-fully-open-transparent-multilingual-lang.

[13] *International Shoe, supra* note 10.

[14] The "purposeful availment" doctrine derives from the Supreme Court's decision in *Hanson v Denckla*, 357 US 235 (1958), which held that due process requires that a defendant "purposefully avail [] itself of the privilege of conducting activities within the forum State." The doctrine was refined in *World-Wide Volkswagen Corp v Woodson*, 444 US 286 (1980), and *Burger King Corp v Rudzewicz*, 471 US 462 (1985). For internet-specific application, see *Zippo Mfg Co v Zippo Dot Com, Inc*, 952 F Supp 1119 (WD Pa 1997).

[15] *Zippo Manufacturing Co. v Zippo Dot Com, Inc.*, 952 F. Supp. 1119, 1124–26 (W.D. Pa. 1997).
(Establishing the influential "sliding scale" framework under which personal jurisdiction is assessed based on the interactivity and commercial nature of a defendant's website, ranging from passive informational sites to highly interactive platforms conducting business with forum residents.) See also: *ALS Scan, Inc. v Digital Service Consultants, Inc.*, 293 F.3d 707, 713–15 (4th Cir. 2002). (Adopting and refining Zippo by holding that jurisdiction exists where a defendant directs electronic activity into the forum with the manifest intent of engaging in business or interactions there.) Although later Supreme Court decisions emphasize defendant-focused contacts, lower courts continue to rely on Zippo-style analysis to assess interactive online services.

[16] *Calder v Jones*, 465 US 783, 789–90 (1984). (Holding that personal jurisdiction may be exercised where a defendant commits an intentional act expressly aimed at the forum state, knowing that the brunt of the harm will be felt there.) See also: *Walden v Fiore*, 571 US 277, 287–90 (2014). (Clarifying that the Calder test requires forum-directed conduct by the defendant itself, not merely foreseeable effects experienced by the plaintiff.)

[17] *International Shoe, supra* note 10. (Foundational standard: minimum contacts assessed under the totality of circumstances, not physical presence.)

[18] *Ford Motor Co. v Montana Eighth Judicial District Court*, 592 US 351, 360–66 (2021).
(Systematically serving a US market through customers and commercial relationships supports jurisdiction.)

[19] *Licci ex rel. Licci v Lebanese Canadian Bank, SAL*, 732 F.3d 161, 170–73 (2d Cir. 2013). (Repeated use of US financial infrastructure, including US-dollar transactions, constitutes purposeful availment.)

[20] *Mavrix Photo, Inc. v Brand Technologies, Inc.*, 647 F.3d 1218, 1229–31 (9th Cir. 2011).
(Targeted advertising and monetization of a US audience support personal jurisdiction.)

[21] *Burger King Corp. v Rudzewicz*, 471 US 462, 473–76 (1985). (Purposeful availment may be established through contracts governed by US law and deliberate affiliation with the forum.)

[22] *ALS Scan, Inc. v Digital Service Consultants, Inc.*, 293 F.3d 707, 713–15 (4th Cir. 2002); *Zippo Manufacturing Co. v Zippo Dot Com, Inc.*, 952 F. Supp. 1119, 1124–26 (W.D. Pa. 1997).
(Jurisdiction based on intentional online activity and interactive services directed at a US audience.)

[23] *Walden v Fiore*, 571 US 277, 284–90 (2014); Cochrane, "Hiding in the Eye of the Storm Cloud,"195–201. (Jurisdiction focuses on the defendant's own contacts with the forum; applied in CLOUD Act context to foreign providers.)

[24] *Briesch v Automobile Club of Southern California*, 40 F. Supp. 2d 1318, 1322–23 (D. Utah 1999) (holding that where a federal statute authorizes nationwide service of process, the relevant inquiry is whether the defendant has minimum contacts with the United States as a whole); *SEC v Knowles*, 87 F.3d 413, 417 (10th Cir. 1996).

[25] *Go-Video, Inc. v Akai Electric Co.*, 885 F.2d 1406, 1415–16 (9th Cir. 1989) (adopting national-contacts analysis under the Fifth Amendment in federal statutory cases).

[26] *In re Tribune Co.*, 418 B.R. 116, 129–30 (Bankr. D. Del. 2009) (describing Fifth Amendment due process as a "general fairness test" incorporating International Shoe but applied to national contacts); *Charan Trading Corp. v Uni-Marts, LLC (In re Uni-Marts, LLC)*, 399 B.R. 400, 406 (Bankr. D. Del. 2009).

[27] *Haile v Henderson National Bank*, 657 F.2d 816, 824–25 (6th Cir. 1981) (recognizing Congress's authority to provide for national service of process and jurisdiction based on nationwide contacts); *Medeco Security Locks, Inc. v Fichet-Bauche*, 568 F. Supp. 405, 408–09 (W.D. Va. 1983).

[28] Stephen E. Sachs, "How Congress Should Fix Personal Jurisdiction," 108 *Harvard Law Review* 1301, 1316–22 (2019); Cochrane, "Hiding in the Eye of the Storm," 186–94.

[29] Cochrane, *supra* note 10 at 153, 186–94.

[30] *Briesch v Automobile Club of Southern California*, 40 F. Supp. 2d 1318, 1322–23 (D. Utah 1999); *SEC v Knowles*, 87 F.3d 413, 417 (10th Cir. 1996) (holding that where a federal statute authorizes nationwide service of process, Fifth Amendment due process turns on contacts with the United States as a whole).

[31] Stephen E. Sachs, "How Congress Should Fix Personal Jurisdiction," 108 *Harvard Law Review* 1301, 1316–22 (2019).

[32] *Go-Video, Inc. v Akai Electric Co.*, 885 F.2d 1406, 1415–16 (9th Cir. 1989); *Haile v Henderson National Bank*, 657 F.2d 816, 824–25 (6th Cir. 1981).

[33] In re Tribune Co., 418 B.R. 116, 129–30 (Bankr. D. Del. 2009); *Charan Trading Corp. v Uni-Marts, LLC (In re Uni-Marts, LLC)*, 399 B.R. 400, 406 (Bankr. D. Del. 2009).

[34] Cochrane, *supra* note 10 at 186–94.

[35] Sachs, "How Congress Should Fix Personal Jurisdiction."

[36] US DOJ, *supra* note 1 at 3. ("The [CLOUD] Act does not create any new legal rights for the U.S. government to access data... When a qualifying foreign government's order seeks data stored in the United States, providers must comply only if doing so would not cause them to violate the laws of the United States, including the Fourth and Fifth Amendment protections of the U.S. Constitution."

[37] Cochrane, *supra* note 10 at 187. Cochrane argues that "it is seriously questionable whether the Due Process Clause imposes any meaningful restrictions" on CLOUD Act jurisdiction over foreign service providers. See also Anthony J. Colangelo, "A Unified Approach to Extraterritoriality" (2011) 97 *Virginia Law Review* 1019 at 1107 ("[I]t is far from clear that Fifth Amendment due process even cares about other nations' sovereignty interests.").

[38] Tim Cochrane, "Digital Privacy Rights and CLOUD Act Agreements," 47 *Brooklyn Journal of International Law* 1, 185–201 (2021). ("This article critiques this belief, examining the impact of CLOUD Act agreements at public and private international law, as well as domestic US and UK law. While the removal of conflicts is a significant private international law benefit itself, CLOUD Act agreements also allow signatory states to significantly expand enforcement jurisdiction over overseas providers at public international law.").

[39] Stephen E. Sachs, "The Unlimited Jurisdiction of the Federal Courts" (2021) 106 *Virgina Law Review* 1703 at 1728-29 ("In general, Congress can extend the federal courts' personal jurisdiction as far as it wants..."). See discussion in Cochrane, "Hiding in the Eye of the Storm Cloud," supra note 10 at 195–98.

[40] *Daimler AG v Bauman*, 571 US 117 (2014); *Bristol-Myers Squibb Co. v Superior Court*, 582 US 255 (2017) (narrowing specific jurisdiction to claims arising from or related to defendant's forum contacts)

[41] See *United States v Verdugo-Urquidez*, 494 US 259 (1990) (declining to extend Fourth Amendment protections to non-resident aliens abroad); *Boumediene v Bush*, 553 US 723 (2008) (extending *habeas corpus* but through a functional, context-specific analysis). The application of Fifth Amendment due process constraints to foreign persons in the CLOUD Act context remains largely untested.

[42] Albert Gidari, "The Big Interception Flaw in the US-UK Cloud Act Agreement," Stanford Law School Center for Internet and Society (October 2019), https://cyberlaw.stanford.edu/blog/2019/10/big-interception-flaw-us-uk-cloud-act-agreement.

[43] See *United States v Denman*, 100 F.3d 399 (5th Cir. 1996); Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010).

[44] *Ford Motor Co. v Montana* Eighth Judicial District Court, 141 S. Ct. 1017, 1036–39 (2021) (Gorsuch, J., concurring). Justice Alito similarly questioned "whether the case law we have developed... is well suited for the way in which business is now conducted." Ibid. at 1032 (Alito, J., concurring). See Cochrane, "Hiding in the Eye of the Storm Cloud," 199-200.

[45] See Cochrane, *supra* not 10 at 199-200.

[46] Rogers Communications Inc. (RCI), Form 20-F Annual Report (2024), filed with the US SEC (disclosing US stock exchange listing and institutional ownership); SEC Form 13F Filings, Q3 2025 (reporting substantial US institutional holdings). See also Rogers Communications Inc., Management Information Circular (2025) at 12–14 (detailing shareholding structure and US investor composition).

[47] BCE Inc., Form 20-F Annual Report (2024), filed with the US SEC.

[48] TELUS Corporation, Form 20-F Annual Report (2024), filed with the US SEC.

[49] See Licci, *supra* note 13, at 170–73 (repeated use of US financial infrastructure, including US-dollar transactions, constitutes purposeful availment).

[50] *Burger King, supra* note 15, at 473–76.

[51] BCE Inc., "BCE Completes Acquisition of Ziply Fiber," news release (August 1, 2025), https://www.bce.ca/news-and-media/releases/show/BCE-completes-acquisition-of-Ziply-Fiber; BCE Inc., Form 20-F Annual Report (2025), filed with the US SEC (reporting acquisition value of approximately US$3.6 billion).

[52] TELUS Corporation, "TELUS Completes Acquisition of Remaining TELUS Digital Shares," news release (September 2025), https://www.telus.com/en/about/news-and-events/media-releases; TELUS Corporation, Form 20-F Annual Report (2025), filed with the US SEC.

[53] TELUS Corporation, Form 20-F Annual Report (2024), filed with the US SEC (disclosing TELUS Digital's US subsidiary operations and employee count); TELUS Digital, "About Us," https://www.telusinternational.com/about (describing the US operational footprint including its Las Vegas headquarters and over 1,600 US employees).

[54] TELUS Digital, "TELUS Digital Announces Acquisition of Gerent," news release, May 28, 2025.

[55] Rogers Communications Inc., Form 20-F Annual Report (2024), filed with the US SEC. For institutional ownership data, see SEC Form 13F filings by major US institutional investors.

[56] Shopify Inc., Form 10-K Annual Report (2024), filed with the US SEC, at 1 (noting transfer of listing to NASDAQ Global Select Market effective March 31, 2025); NASDAQ, "NASDAQ-100 Index Annual Changes," news release (May 19, 2025) (announcing Shopify's addition to the NASDAQ-100).

[57] Shopify Inc., *supra* note 56, at 38 (reporting gross merchandise volume of US$292.3 billion for fiscal 2024, with approximately 57 percent processed in the United States).

[58] Shopify Inc., *supra* note 56, at 28 (listing principal executive offices in Ottawa, Ontario and noting US operational presence); Shopify Inc., "About Shopify," https://www.shopify.com/about (describing global operations including US headquarters functions).

[59] Shopify Inc., *supra* note 56, Exhibit 21.1 (List of Subsidiaries), filed with the US SEC (identifying US subsidiaries including Shopify Data Processing (USA) Inc., Shopify Payments (USA) Inc., and Shopify Holdings (USA) 2 Inc.).

[60] BNN Bloomberg, "Canada Tech Firm Shopify Fuels Fear of US Move with Filing Change," February 28, 2025; TD Securities Inc., Research Note, February 2025 (analyzing Shopify's 10-K filing).

[61] See *Briesch, supra* note 24, at 1322–23; See SEC, *supra* note 18, at 417.

[62] See *Gucci America, supra* note 9; Justin Hemmings, Sreenidhi Srinivasan and Peter Swire, "Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the CLOUD Act," 10 *Journal of National Security Law & Policy* 631 (2020).

[63] French Senate, "Commande publique: audition de Microsoft," (June 10, 2025).

[64] *United States v Microsoft Corp*., 138 S. Ct. 1186 (2018) (per curiam) (dismissing case as moot following passage of the CLOUD Act). See also Jennifer Daskal, "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0," (2019) 71:9 *Stanford Law Review 9*.

[65] Treaty between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters, March 18, 1985, Can TS 1990 No 19.

[66] *R v Spencer,* 2014 SCC 43; *R v Bykovets*, 2024 SCC 6 (affirming judicial gatekeeping and reasonable expectation of privacy in third-party-held data).

[67] Barry Appleton, "Whose Law Governs Canadian Data?" (2025) at Part 5; Citizen Lab, "Canada-U.S. Cross-Border Surveillance Negotiations Raise Constitutional and Human Rights Concerns," (2025).

[68] 18 USC § 2713; *United States v Microsoft, supra* note 64 (mootness following enactment).

[69] Public Safety Canada, "The U.S. and Canada Reestablish the Cross-Border Crime Forum" (March 22, 2022).

[70] Khoo and Robertson, "Canada-U.S. Cross-Border Surveillance Negotiations."

[71] *Gucci America, supra* note 9; *In re Grand Jury Investigation of Possible Violations* of 18 USC § 1956 & 50 USC § 1705, 381 F. Supp. 3d 37 (D.D.C. 2019), aff'd sub nom. *In re Sealed Case,* 932 F.3d 915 (D.C. Cir. 2019).

[72] Hemmings, Srinivasan & Swire, *supra* note 62, 2, 631–90.

[73] Cochrane, *supra* note 10 at 153–208.

[74] *R. v Spencer* and *R. v Bykovets supra* note 66.

[75] Congressional Research Service, *Law Enforcement Access to Overseas Data Under the CLOUD Act* (LSB10125).

[76] French Senate, *supra* note 63; Appleton, *Clause & Effect* (July 21, 2025).

[77] *In re Grand Jury Proceedings* (Bank of Nova Scotia), 691 F 2d 1384 (11th Cir 1982); 740 F 2d 817 (11th Cir 1984).

[78] 18 USC § 2703(h) (motion to quash or modify based on "qualifying foreign government" conflict); Restatement (Third) of the Foreign Relations Law of the United States §442. (1987).

[79] *Société Nationale Industrielle Aérospatiale v United States District Court*, 482 US 522 (1987) (comity/balancing in cross-border evidence disputes).

[80] French Senate, *supra* note 63.

[81] Coverage includes: "Microsoft tells French lawmakers it can't protect user data from US demands" *SDxCentral* (July 21, 2025); "Microsoft exec admits it 'cannot guarantee' data sovereignty" *The Register*, (July 25, 2025).

[82] Barry Appleton, "The Cloud Casts a Long Shadow: Microsoft, the CLOUD Act, and Canada's Vanishing Digital Sovereignty" *Appleton's Clause & Effect* (21 July 2025), https://barryappleton.substack.com/p/the-cloud-casts-a-long-shadow.

[83] Appleton, "The Cloud Casts a Long Shadow."

[84] *In Re Grand Jury Proceedings* (Bank of Nova Scotia), *supra* note 77.

[85] See *Restatement (Third) of the Foreign Relations Law of the United States* § 442 (1987); *Société Nationale Industrielle Aérospatiale v United States District Court*, 482 US 522 (1987); *United States v First National City Bank*, 396 F 2d 897 (2d Cir 1968).

[86] *Smith v Maryland*, 442 US 735 (1979).

[87] *R. v Spencer, supra* note 66.

[88] *R. v Bykovets, supra* note 66.

[89] See *R v Love*, 2022 ABCA 269, https://canlii.ca/t/jqpsr; Citizen Lab, "Canada-U.S. Cross-Border Surveillance Negotiations."

[90] The US third-party doctrine holds that individuals have no reasonable expectation of privacy in information voluntarily conveyed to third parties. This doctrine enabled warrantless surveillance of metadata and business records until partially limited by *Carpenter v United States*, 585 US 296 (2018).

[91] Cochrane, "Digital Privacy Rights," examining the Fourth Amendment and ECHR Article 8 implications of CLOUD Act executive agreements.

[92] US DOJ, Report to Congress on the Implementation of the US-UK CLOUD Act Agreement (November 2024), https://www.documentcloud.org/documents/25551978-doj-report-to-congress-on-us-uk-cloud-act-agreement/.

[93] Richard Salgado, "First Insights Into the US-UK CLOUD Act Agreement," *Lawfare* (March 10, 2025), https://www.lawfaremedia.org/article/first-insights-into-the-u.s.-u.k.-cloud-act-agreement. See also Greg Nojeim, Testimony before the House Judiciary Committee, Subcommittee on Crime and Federal Government Surveillance (June 5, 2025), https://www.congress.gov/119/meeting/house/118335/witnesses/HHRG-119-JU08-Wstate-NojeimG-20250605.pdf

[94] US DOJ Report to Congress, *supra* note 92. The statistics on requests are on pages 5-6 of the DOJ Report.

[95] Salgado, *supra* note 93 ("the U.K. has continued to use the MLAT process at the same rate as before the CLOUD Act").

[96] Salgado, *supra* note 93..

[97] Public Safety Canada, Briefing Materials on Canada-US CLOUD Act Negotiations (2022–2024) (describing executive agreement as addressing delays in electronic evidence production and emphasizing "timely and effective" investigative access).

[98] Public Safety Canada, "The U.S. and Canada Reestablish the Cross-Border Crime Forum," news release, March 22, 2022, https://www.canada.ca/en/public-safety-canada/news/2022/03/the-us-and-canada-reestablish-the-cross-border-crime-forum.html.

[99] Osler, Hoskin & Harcourt LLP, "Data Sovereignty in Light of the CLOUD Act: Back to the Future?," October 7, 2025, https://www.osler.com/en/insights/updates/data-sovereignty-in-light-of-the-cloud-act-back-to-the-future/ ("Canada has been negotiating a CLOUD Act agreement with the U.S. since 2022, but no agreement is currently in place").

[100] Khoo and Robertson, "Canada-U.S. Cross-Border Surveillance Negotiations."

[101] International Centre for Criminal Law Reform, "Canada's Future CLOUD Act Agreement with the United States," March 29, 2022, https://icclr.org/2022/03/29/canadas-future-cloud-act-agreement-with-the-united-states/.

[102] Canadian Bar Association, Privacy and Access Law Section, *Submission on a Potential Canada–U.S. CLOUD Act Agreement* (November 2024) at 3–5 (MLAT preservation), 6–7 (government data exemptions), 9–11 (judicial review), 12–14 (privacy-law amendments), https://nationalmagazine.ca/en-ca/articles/cba-influence/submissions/2025/how-to-address-canada-s-digital-data-disclosures-with-the-u-s.

[103] Canadian Civil Liberties Association, "CCLA and coalition of coalitions call for withdrawal of Bill C-2" (July 14, 2025), https://ccla.org/privacy/ccla-joins-calls-for-withdrawal-of-bill-c-2/.

[104] Joseph Menn, "U.K. Orders Apple to Let It Spy on Users' Encrypted Accounts," *The Washington Post*, February 7, 2025, https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/; Joseph Menn, "Apple Yanks Encrypted Storage in U.K. Instead of Allowing Backdoor Access," *The Washington Post*, February 21, 2025, https://www.washingtonpost.com/technology/2025/02/21/apple-yanks-encrypted-storage-uk-instead-allowing-backdoor-access/.

[105] *In re Apple, Inc.*, No. 15-mc-1902 (E.D.N.Y. February 29, 2016); see also Matt Apuzzo and Joseph Goldstein, "Apple Fights Order to Unlock San Bernardino Gunman's iPhone," *The New York Times*, February 17, 2016.

[106] CLOUD Act, US DOJ, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (Washington, DC: US DOJ, April 2019), 9–11; Jennifer Daskal, "Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0," *Stanford Law Review Online* 71 (May 2018): 9–48.; BSA | The Software Alliance, "The U.S. CLOUD Act: Myths vs. Facts," April 2019.

[107] US Department of the Treasury, "Treasury Sanctions Company Associated with Salt Typhoon" (January 17, 2025), https://home.treasury.gov/news/press-releases/jy2792; Congressional Research Service, "Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications" (January 23, 2025), https://www.congress.gov/crs-product/IF12798.

[108] The White House, *supra* note 2 at 18-19..

[109] The White House, *supra* note 2 at 18-19.

[110] The White House, *supra* note 3.

[111] The White House, *supra* note 3 at i.

[112] Atlantic Council, "Inside the Trump trade strategy with US Trade Representative Jamieson Greer" Transcript (10 December 2025), https://www.atlanticcouncil.org/news/transcripts/inside-the-trump-trade-strategy-with-us-trade-representative-jamieson-greer/

[113] Barry Appleton, "Law, Not Leverage: A Rules-Based Path for the USMCA Review—Rebuttal Comments to the US Trade Representative" Docket No. USTR-2025-0004 (December 12, 2025), https://ssrn.com/abstract=5668791.

[114] Appleton, "Law, Not Leverage."

[115] *Foreign Extraterritorial Measures Act*, RSC 1985, c F-29, s 3.

[116] *Foreign Extraterritorial Measures Act*, RSC 1985, c F-29, s 3.

[117] See Norton Rose Fulbright, "Between a rock and a hard place: Canadian companies face increased risks following US decision to implement Title III right of action," (2019), https://www.nortonrosefulbright.com/en/knowledge/publications/60af4e56/between-a-rock-and-a-hard-place-canadian-companies-face-increased-risks-following.

[118] FEMA, s 7(3).

[119] Certain Foreign Extraterritorial Measures (United States) Order, 2014, SOR/2015-12.

[120] US DOJ, Report to Congress, *supra* note 92 , revealing that the United Kingdom issued over 20,000 requests to US providers in two years, overwhelmingly for interception rather than stored data.

[121] Khoo and Robertson, "Canada-US Cross-Border Surveillance Negotiations."

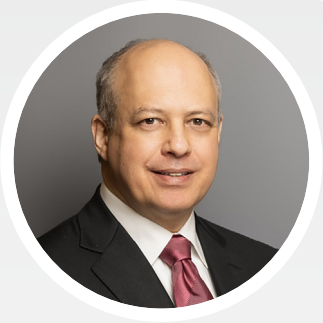
[122] *Foreign Extraterritorial Measures Act, supra* note 116, (authorizing orders prohibiting compliance with foreign measures that adversely affect Canadian interests or infringe Canadian sovereignty).

[123] *In Re Grand Jury Proceedings* (Bank of Nova Scotia), 691 F.2d 1384 (11th Cir. 1982); 740 F.2d 817 (11th Cir. 1984) (enforcing subpoenas despite foreign blocking statutes and imposing substantial fines for non-compliance).

[124] Treasury Board of Canada Secretariat, *supra* note 6.

[125] Privacy Commissioner of Canada, *supra* note 8.

[126] Menn, "U.K. Orders Apple to Let It Spy"; Congressional Research Service, "Salt Typhoon Hacks."



Barry Appleton is a scholar and fellow at the Balsillie School of International Affairs. He is also the co-director and distinguished senior fellow at the Center for International Law at the New York Law School. Prof. Appleton is a highly regarded authority on the convergence of international trade, intellectual property, international economic law, and digital governance. He is the author of two books on the NAFTA and publishes extensively on how digital privacy, AI, digital platforms, blockchain, and trade redefine sovereignty and law. An acclaimed commentator and educator, he advocates for democratic rules-based frameworks in the algorithmic age.

BALSILLIE PAPERS

ISSN 2563-674X • doi:10.51644/BAP97

balsilliepapers.ca