Canadian Data Protection and Cybersecurity in an Era of Diminishing North American Cooperation

Muna Mohamed and Ananya Vohra

Issue

Canada must urgently strengthen domestic data security and restrict cross-border data flows to the United States, where weak data protection laws threaten Canadian sovereignty, economic competitiveness and digital security.

Background

Digital Sovereignty

In an increasingly digitized world, where nearly every aspect of life is mediated by technology, data has become an essential resource (Ciuriak 2024). Data informs decision making, powers innovation in varies technologies such as artificial intelligence (AI) and gives firms and governments a competitive edge. Global value chains also rely on fast, reliable access to data to keep operations running smoothly (Leblond and Aaronson 2019).

Digital sovereignty refers to a state's ability to control its own digital infrastructure, including data, hardware and software, with many policies focused on achieving self-sufficiency (Larsen 2022). Currently, 92 percent of data from users in the Global North is stored on servers owned by US-based tech companies, consolidating much of the jurisdictional authority within a single country (Fleming 2021).

Although much of Canada's data is stored on servers in the United States, neither country has established comprehensive laws or guidelines to protect this data (Orr 2019). Additionally, there are no specific regulations that require data to be stored within Canada, and the dominance of US-based technology providers such as Google have contributed to a growing reliance on American cloud services (ibid.). The absence of robust data protections and digital sovereignty increases the likelihood of data being weaponized. As Xuan Liu (2022,) notes, "Data is the strategic intelligence of a country, and the party with the advantage of data can carry out 'dimensionality reduction' strikes." Data impacts national security in three keys ways:

- **Undermining democratic institutions:** Data on specific demographics can allow algorithms to send misinformation and target specific people (Dawood 2021, 10–31).
- **Crippling critical infrastructure:** Without proper regulations, hackers can aid terrorists and hostile states in accessing critical information about Canadian critical infrastructure (information on roads, pipelines, electricity grids, health care, etc.)
- **Big tech control of cloud computing:** The Canadian and US governments regularly collaborate with big tech and depend on commercial communication and cloud services. However, the profit-driven nature and lack of public accountability of these companies pose risks of sensitive data being misused or accessed by adversaries (Schaake 2024).

Without strong policies guiding data protection, big tech often fails to address software vulnerabilities, making them susceptible to cyberattacks (ibid.). Despite these risks, there is currently little organizational structure beyond the security measures tech companies implement internally to mitigate such threats (ibid.).

Data protection regulations typically establish rights to access, deletion and portability of data, while mitigating risks and shielding individuals from potential threats (Kira, Sinha and Srinivasan 2021, 1337–60). Data localization is a key mechanism for enhancing data protection and digital sovereignty. It refers to policies requiring that data generated within a country be stored and processed on domestic servers or within cloud environments operated by entities physically located and regulated within national borders (Trachtenberg 2025, 1–3). In Canada's case, this would mean ensuring Canadian data remains within Canadian data centres. Canada's lack of comprehensive data localization policies, combined with limited domestic internet and data infrastructure, results in a heavy reliance on US networks. This creates a phenomenon known as "boomerang routing," whereby Canadian data routinely passes through the United States, even when users access domestic websites (Orr 2019). Although most American trade agreements, such as the Canada-United States-Mexico Agreement (CUSMA), include commitments to protecting personal information (Trachtenberg 2025, 1–3), they do not address data related to national security. Once data crosses into the US, it is subject to US jurisdiction, where there are no comprehensive federal data protection laws. This exposes Canadian data to potential misuse and significantly weakens Canada's ability to safeguard its digital sovereignty and uphold national privacy standards.

Evolving US-Canada Dynamics

The new Trump administration's approach to data access presents challenges to Canadian digital sovereignty, highlighting the need for careful consideration of data-sharing policies. The United States has traditionally emphasized openness and minimal regulation in its approach to data governance (Hollis and Raustiala 2022). Under the Biden administration, however, there was a gradual shift toward stronger data and AI regulations aimed at protecting national security, as reflected in measures such as *the Protecting Americans' Data from Foreign Adversaries Act of 2024* and the Protecting Americans from Foreign Adversary Controlled Applications Act of 2024. In contrast, President Trump's second presidency has largely advocated for deregulation to accelerate innovation in strategic sectors like AI (InCountry 2025). Without strong domestic safeguards and infrastructure, Canadian data remains vulnerable to US policy shifts.

Recent actions by the Trump administration have strained historically close US-Canada relations and heightened concerns about the security of Canadian data, particularly as the United States intensifies efforts to advance AI (Al-Haque et al. 2024). Canada holds some of the world's most comprehensive and representative datasets, which are vital for training effective and equitable AI systems. Health data is a prime example: Canada's centralized, publicly funded health-care system generates inclusive data that captures a wide demographic range (ibid.). In contrast, the United States' fragmented, insurance-based system creates significant data gaps by excluding uninsured populations (Canadian Press 2025). This highlights the strategic value of Canadian data and the need to safeguard it. However, much of this data is stored by American tech companies such as Microsoft, Google and Amazon Web Services (ibid.). With diplomatic relations under strain and the US government showing little regard for Canadian sovereignty, legal experts and medical researchers are increasingly concerned that Canadian health data could be accessed or used by the United States without Canadian consent. All three companies have confirmed that they would comply with lawful US court orders, even if doing so conflicts with Canadian interests (ibid.).

Implementing strong data protection measures would not only shield Canada from cyber threats but also contribute to national defence efforts, which are also a focus of the US administration. President Trump has repeatedly emphasized the need for Canada to increase its defence spending to meet the two percent North Atlantic Treaty Organization target (Wherry 2024). By prioritizing data security, Canada can demonstrate its commitment to security and cooperation with its allies. Investment into cybersecurity and data protection gives Canada the opportunity to build a strong industrial base and skilled workforce that is ready to handle emerging technological challenges. This would also enable Canada to become a global expert on cybersecurity, making us indispensable to our allies. Within the defence realm, a number of new threats to national security and sovereignty require new thinking toward defence and defence capability. Increasingly, national defence has come to include economic security (National Defence 2024). Ensuring economic prosperity requires not only reliable cybersecurity systems and internet infrastructure, but also strategic control over data. While curated data can be shared with US partners to strengthen cross-border collaboration, the Canadian government must retain authority over how that data is used and disseminated. This raises key questions about which data Canada should safeguard, and which data can be leveraged in negotiations with the United States.

It should also be noted that Canada's data relationship with the United States is shaped by both formal agreements and operational practices that facilitate the automatic sharing of personal information of persons within their borders. Under existing protocols, Canada and the United States exchange biographic and biometric data on non-citizens and permanent residents (Nardi 2025). For example, Canada is authorized to use information about US permanent residents applying for immigration to Canada to query their immigration history with US authorities. The United States can, in turn, access similar data on Canadian permanent residents (ibid.). Additionally, in CUSMA, Article 19.12 reinforces the free flow of data across borders by prohibiting barriers to cross-border data transfers among the three countries. While this facilitates trade and integration, it also limits Canada's ability to impose stronger data protection requirements on information that leaves its jurisdiction.

Current Canadian Data Protection Measures

Within its own borders, Canada lacks comprehensive and enforceable legislation governing data, especially cross-border data flows. Existing laws like the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA) offer general protections for personal data held by federal institutions and private entities (Office of the Privacy Commissioner of Canada n.d.). Specifically, PIPEDA establishes the foundational rules for collecting, using and disclosing personal information, while also granting individuals the right to access and control their own data (ibid.). However, as previously noted, Canada's digital infrastructure relies heavily on the United States due to boomerang routing, meaning Canadian data is no longer protected once it exits national jurisdiction. At the provincial level, Alberta, British Columbia and Quebec have enacted privacy legislation that addresses some aspects of digital governance. However, there are no existing federal or provincial laws that provide a full regulatory framework tailored to the new unique challenges posed by AI technologies.

Ontario has taken a step forward with Bill 194, which aims to modernize digital security and privacy practices in the public and private sector. The bill's Section 2 amends the Freedom of Information and Protection of Privacy Act, requiring institutions to conduct privacy impact assessments and report breaches that pose a real risk of significant harm (Legislative Assembly of Ontario 2024). Bill 194 also expands the powers of the Privacy Commissioner to ensure compliance and protect citizens' digital rights (ibid.). While this bill marks progress at the provincial level, it further illustrates the fragmented nature of Canada's digital governance landscape. The federal government took steps toward modernizing its approach to AI and data regulation with the introduction of the Artificial Intelligence and Data Act. However, the bill was not passed due to the prorogation of Parliament earlier in 2025, and it will now be up to the new parliamentary session to revisit and advance.

National defence is one of the few areas where the federal government is actively developing policy on data. Canada's most recent national defence policy outlines a commitment to advancing big data capabilities, acquiring sophisticated analytical technologies and enhancing secure cloud-based computing (National Defence 2024). These digital initiatives aim to build a data-driven defence organization that can rapidly transform information into actionable insights, enabling faster decision making and near real-time responses (ibid.). However, these advancements are primarily focused on data relevant to the Canadian Armed Forces, with limited attention given to other forms of data that may also pose risks to national or economic security.

Canada is at a crossroads: whether to align with the US model of minimal data regulation or the European Union's stricter, privacy-focused approach. Regardless of the choice, Canada must ensure it has a strong voice in shaping international data rules to protect its sovereignty and national interests.

Key Partnerships

To implement effective data protection regulations, Global Affairs Canada (GAC) should consider working closely with key federal agencies on regulating data flows. One of the most important of these agencies is the Innovation, Science and Economic Development Agency (ISED). The ISED plays a critical role in Canada's technology development and digital infrastructure, making it an essential player in any efforts related to data sovereignty and security. The ISED will be crucial in advancing a national strategy focused on protecting Canadian data and ensuring its sovereignty. This includes developing the infrastructure necessary to secure data and support policies that protect Canada's interests in an increasingly digital world. With the ISED's expertise, GAC can help shape a robust framework that aligns with Canada's digital and economic goals.

In addition, GAC should partner with the Communications Security Establishment (CSE), particularly through its Canadian Centre for Cyber Security, also known as the Cyber Centre. As the federal government's technical authority on cybersecurity, the Cyber Centre leads Canada's response to cybersecurity incidents and provides expert guidance to protect the systems and information Canadians rely on every day. It also has a track record for working with other levels of government and critical infrastructure operators to safeguard the digital foundations of Canada's economy and society (Government of Canada 2023). Leveraging the CSE's technical capabilities would enhance Canada's ability to protect sensitive data, respond to cyber threats and support GAC's ability to secure implementation of international digital policy.

Recommandations

Implement a data location tier. To strengthen Canada's digital sovereignty and security, the federal government should implement a policy of "tiering data" based on its sensitivity. This approach would involve categorizing data according to its potential risks to national security, privacy and economic stability, allowing for more tailored and secure storage solutions. High-sensitivity data that can impact national security — such as information related to personal, demographic and health — should be stored in secure, domestic environments, while less sensitive data could continue to flow with fewer restrictions. By organizing data in this manner, Canada can better allocate resources, enhance data protection measures and ensure that critical information remains safeguarded while allowing for efficient handling of less critical data. To achieve this, the federal government must collaborate with agencies such as the CSE to develop a regulatory framework that clearly defines which types of data must remain within national jurisdiction.

Investment into digital infrastructure. The federal government should prioritize building robust Canadian digital infrastructure, including secure, Canadian-owned data centres, expanded power grid capacity and sovereign cloud services, to reduce reliance on foreign networks and strengthen national control over data. A tiered data localization strategy should guide this investment, ensuring highly sensitive data remains in Canada while encouraging voluntary domestic retention of less sensitive data. Rather than imposing strict localization laws, which risk deterring US investment or straining Canada-US relations, the government should offer incentives for Canadian firms to store and process data within national borders. This dual approach would safeguard digital sovereignty, stimulate the domestic digital economy and enable Canada to assert greater control over its data while remaining interoperable with trusted international partners.

Add cybersecurity experts to GAC's US team. Lastly, as trade negotiations with the United States increasingly touch on issues of digital infrastructure and data governance, it is essential that GAC integrates cybersecurity experts into its US-Canada relations team. Canadian data is both abundant and highly valuable, and its protection is vital to the country's economic growth, innovation potential and national security. In today's digital landscape, where cyberthreats can compromise not only sensitive information but also the integrity of diplomatic and economic agreements, expert oversight is indispensable. Cybersecurity professionals can proactively identify and mitigate vulnerabilities that may be overlooked during high-level negotiations. Moreover, they can evaluate the strategic risks posed by proposals that offer greater access to Canadian data in exchange for reduced trade barriers, ensuring that such concessions do not compromise national interests. A dedicated expert would also play a critical role in shaping cross-border, data-sharing frameworks to align with Canada's privacy legislation, cybersecurity standards and long-term geopolitical objectives. Such expert capability would help safeguard Canadian sovereignty in the digital realm and reinforce public trust in international agreements.

About the Authors

Muna Mohamed is a student in the University of Waterloo's Master of Arts in Global Governance program, based at the Balsillie School of International Affairs.

Ananya Vohra is a student in the University of Waterloo's Master of Arts in Global Governance program, based at the Balsillie School of International Affairs,

Acknowledgements

The authors would like to thank Professor Debora Van Nijnatten and Professor Ann Fitz-Gerald for their guidance and mentorship throughout the course of the fellowship program.

Works Cited

Al-Haque, Shahed, Marie-Renée B-Lajoie, Erez Eizenman and Nick Milinkovich. 2024. "The Potential Benefits of AI for Healthcare in Canada." McKinsey & Company, February 26. www.mckinsey.com/industries/healthcare/our-insights/the-potential-benefits-of-ai-for-healthcare-in-canada.

Ciuriak, Dan. 2024. "The Investment Canada Act: Updates for the Knowledge-Based and

Data-Driven Economy at the Dawn of the Age of Machine Knowledge Capital." Brief. http://dx.doi.org/10.2139/ssrn.4771331.

Dawood, Yasmin. 2021. "Combatting Foreign Election Interference: Canada's Electoral Ecosystem Approach to Disinformation and Cyber Threats." *Election Law Journal,* 20(1). https://doi.org/10.1089/elj.2020.0652.

Fleming, Sean. 2021. "What is Digital Sovereignty and Why is Europe so Interested in it." World Economic Forum, January 10. www.weforum.org/stories/2021/03/europe-digital-sovereignty/.

Government of Canada. 2023. "About the Cyber Centre." Canadian Centre for Cyber Security. www.cyber.gc.ca/en/about-cyber-centre.

Hollis, Duncan B. and Kal Raustiala. 2022. "The Global Governance of the Internet." In *The Oxford Handbook of International Institutions*, edited by Duncan Snidal and Michael N. Barnnett, Temple University Legal Studies Research Paper No. 2022-17. http://dx.doi.org/10.2139/ssrn.4197418.

InCountry. 2025. "Trump's impact on global data sovereignty." *InCountry* (blog). February 11. https://incountry.com/blog/trumps-impact-on-global-data-sovereignty/.

Kira, Beatriz, Vikram Sinha and Sharmadha Srinivasan. 2021. "Regulating digital ecosystems: bridging the gap between competition policy and data protection." *Industrial and Corporate Change* 30 (5). https://doi.org/10.1093/icc/dtab053.

Larsen, Benjamin Cedric. 2022. "The Geopolitics of AI and the Rise of Digital Sovereignty." The Brookings Institution, December 8. www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/.

Leblond, Patrick and Susan Ariel Aaronson. 2019. *A Plurilateral "Single Data Area" Is the Solution to Canada's Data Trilemma.* CIGI Papers No. 226. Waterloo, ON: Centre for International Governance Innovation. www.cigionline.org/sites/default/files/documents/no.226.pdf.

Legislative Assembly of Ontario. "Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024." https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194.

Liu, Xuan. 2022. "The Study on National Security in Big Data Era." *Frontiers in Business, Economics and Management* 5(3), Article 3. https://doi.org/10.54097/fbem.v5i3.2006.

National Defence. 2024. *Our North, Strong and Free: A Renewed Vision for Canada's Defence*. www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html.

Nardi, Christopher. 2025. "The U.S. and Canada quietly agreed to share personal data on permanent residents crossing the border." *National Post,* January 15. https://nationalpost.com/news/politics/the-u-s-canada-share-personal-data-permanent-residents.

Office of the Privacy Commissioner of Canada. "PIPEDA Requirements in Brief," https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

Orr, Jacqueline. 2019. "Canadian Cross-Border Data: Your Data May Be Heading South Even When You Are Not." Wilson Center Canada Institute, May. www.wilsoncenter.org/sites/default/files/media/documents/article/canadian_cross-border_data_report.pdf.

Schaake, Marietje. 2024. *The Tech Coup: How to Save Democracy from Silicon Valley*. Princeton, NJ: Princeton University Press. https://doi.org/10.2307/jj.13359161.

The Canadian Press. 2025. "Protect 'valuable' Canadian health data from Trump's AI aspirations,

experts urge." CTV News, April 24. www.ctvnews.ca/health/article/protect-valuable-canadian-health-data-from-trumps-ai-aspirations-experts-urge/.

Trachtenberg, Danielle M. 2025. "Digital Trade and Data Policy: Key Issues Facing Congress."

Congressional Research Service, January 6. https://crsreports.congress.gov/product/pdf/IF/IF12347

Wherry, Aaron. 2024. "Everyone agrees Canada should spend more on defence. How do we pay for it?" *CBC News*. https://www.cbc.ca/news/politics/canada-defence-spending-nato-trump-1.7397141