Exploited and Underutilized: Canada's Broken Data Economy

Canadian Shield Institute

Foundations of Digital Sovereignty
Chapter 4 - May 2026

4

Contents

Contact:

Canadian Shield Institute
150 King St. West,
Toronto, Ontario, CA

canadianshieldinstitute.ca
info@canadianshieldinstitute.ca

Authors:

Vass Bednar
James McLeod
David Corbett
Emily Osborne
Kaylie Tiessen
Matthew da Mota

Photography:

James McLeod
Nattipat Vesvarute
Juan Rojas

Overview

Canada's data governance regime is built on legislation that predates smartphones, social media, and generative AI. The result is a broken dynamic: Canadians feel surveilled and exploited by data-driven firms, while vast troves of high-value institutional data sit unorganized and untapped. Foreign companies extract economic value from Canadian data without compensation, while Canada's own institutions lack the tools to mobilize that data for public benefit. This chapter argues for two complementary solutions: modernized data legislation that genuinely protects Canadians, and a national data trust to steward and deploy Canada's data resources in the national interest.

Key Takeaways

1. Canada's primary federal privacy law, PIPEDA, was enacted in 2000 and has not been substantially updated since 2015 — well before generative AI reshaped the data landscape. The Privacy Act that governs government data hasn't been overhauled since it was implemented in 1983.

2. Foreign firms mediate roughly 60% of digital products and services used by Canadians, meaning the economic value extracted from Canadian personal data flows predominantly out of the country.

3. Canada's data is both exploited and underutilized at the same time — Canadians distrust data-driven systems, which blocks the country from capturing the benefits of its own data wealth.

4. A modernized data governance framework should include an updated data privacy law that enacts meaningful opt-out rights, data portability, limits on predatory uses like algorithmic pricing, and strengthened enforcement powers for privacy regulators.

5. A national data trust would consolidate and govern Canada's institutional and proprietary data — health records, research data, and government data — providing principled access for research and innovation while keeping value in Canada.

The Value of Data in the Modern Economy

For Canada to thrive in the 21st century digital economy, we need to build a governance model that asserts our national sovereignty, while also capturing value to generate Canadian prosperity.

In the previous chapter of *Foundations of Digital Sovereignty*, we looked at the importance of owning and governing intellectual property — the novel ideas that result in competitive advantage for innovative companies. We also looked at standards — the most complex and technical form of governance.

Standards can also allow for technologies to interoperate and perform reliably in the marketplace, but if they are weaponized, standards can also tilt the playing field to create a competitive advantage.

Standards shape and regulate the structures of modern technology, and IP represents the ownership of new and innovative ways to commercialize technology. Data, meanwhile, is the basis of all modern technology. However, the current status quo for data is deeply dysfunctional.

Canadians feel targeted and exploited by data-driven firms, while troves of high-value data remains locked away, providing no economic value to Canada.

A better path forward is for Canada to treat data as a strategic national asset and act accordingly.

In practice, this means that the government should enact comprehensive data legislation that rebuilds trust by protecting individuals and institutions from exploitation. At the same time, Canada should establish a national data trust capable of organizing, safeguarding and mobilizing Canada's own data resources.

What is Data?

Data is information. It can be music, or it can be sensor logs from industrial infrastructure. In many cases, data can be a granular record of individuals' lives. It is widely understood that data is enormously valuable in the modern economy, but it is difficult to put an exact number on this value.

Meta, whose entire business is built upon commercializing data, earned $200 billion USD in revenue in 2025[1]; investors value the company at $1.7 trillion USD at the time of writing.

In 2018, Statistics Canada has estimated that Canada's data and data-related assets were worth around $217 billion.[2]

In 2023, data expert Dan Ciuriak estimated that U.S. data is approximately valued at $6 trillion USD.[3]

The reality is the value of data will vary widely depending on the specific context: What information does the data record? How expansive is the data set? Who is in possession of that data set? By what means can the data be used in business?

A day's worth of data from an industrial sensor monitoring the flow rate of an oil pipeline would be of very little value to most people, but it might be extraordinarily valuable to a commodities trader at a Wall Street investment bank.

Opportunities and Risks for Canada's Data

Canada's data landscape is a mess.

Companies collect vast amounts of personal data about Canadians, and use that data in a range of opaque and predatory ways. Canadians' trust in big tech companies is extremely low. Canada's digital economy is valued at about $123 billion annually, however foreign firms mediate approximately 60% of all digital products and services used by Canadians.[4]

That means that when companies extract value through targeted advertising, algorithmic pricing, analytics, and other revenue streams based on Canadian personal data, economic value flows to non-Canadian companies. As foreign companies extract value from Canadian data without compensation, Canada risks ceding not just economic opportunity, but the informational foundations of its own sovereignty.

Meanwhile, Canadian institutions hold massive troves of data — health records, geological and climate data, financial data and more. This data is especially valuable, but it remains both uncategorized and unorganized, leaving it underutilized despite its significant potential worth. It's tough to suggest that the government take steps to derive more economic value from the institutional data that is currently gathering dust on the shelf.

When citizens feel like they are being surveilled and exploited already, how do you convince them to let anybody access something as sensitive as a health record?

AI runs through every dimension of Canada's data challenge as both amplifier and risk. It supercharges beneficial and harmful uses of data alike, and AI development depends on vast training datasets.

Canada faces a pressing risk of uncompensated scraping — Canadian data used to train foreign models that are then sold back to Canadian users, with no compensation or governance over how that data was used.

Canada's Privacy Commissioner found that 83% of Canadians are concerned about privacy when using AI tools, and more than 70% of queries to AI chatbots contained personally identifiable information.[5]

Consent frameworks have not kept pace: users cannot meaningfully agree to future uses of their data that are unknowable at the point of collection. This gap extends to research, where AI systems that give preference to certain sources over others threaten academic independence, and to defence, where algorithmic decision making based on incomplete or improperly captured data can produce unjust and harmful outcomes.

Canada's Current Data Governance Regime

Canada's federal privacy landscape is made up of two pieces of legislation:

- The Privacy Act, for information collected about individuals by the government.[6]
- The Personal Information Protection and Electronic Documents Act (PIPEDA), for personal information collected by the private sector.[7]

PIPEDA was enacted in 2000, and the most recent substantial updates were passed in 2015.[8] The Privacy Act has not been substantially overhauled since it was enacted in 1983. Notably, neither piece of legislation has been modernized since generative AI entered the scene and sharpened the demand for data and need for protection.

As it stands, PIPEDA requires that private sector organizations obtain "meaningful consent" for the collection, use or disclosure of personal information, defined as any information about identifiable individuals.[9] Individuals must understand what they are consenting to and consent may only be required "to fulfil an explicitly specified and legitimate purpose."[10] Consent must be obtained again for any new purpose.

However, PIPEDA's reliance on consent has been critiqued for placing an unrealistic burden on individuals to read long and complex privacy policies.[11] It also raises questions about whether consent can ever be fully informed in a digital context, and often leads to "take-it-or-leave it terms" from organizations.[12]

PIPEDA also has weak compliance initiatives and insufficient enforcement powers.[13] While it gives the Privacy Commissioner the authority to investigate an organization's data handling practices, any real enforcement occurs through an application to the federal court, where processes are duplicated and lengthy before any breach of PIPEDA is confirmed.[14]

When information is de-identified or anonymized such that it no longer meets the definition of personal information, it is no longer covered under PIPEDA.[15]

This raises serious concerns, first and foremost because de-identified data can be re-identified later.[16] PIPEDA's lack of jurisdiction over de-identified data also means that companies can use mass surveillance data collection for any predatory purposes, as long as they are anonymizing the data.

The most recent attempt to amend PIPEDA recognized these risks but placed limits on the reuse of de-identified information, even for socially beneficial purposes, that would have jeopardized innovation.[17]

European Inspiration for Data Legislation

As it stands, Canada's approach to data governance largely follows the American model, which has limited regulation over data collection or usage. This model works well for the United States; it enables large American companies to capitalize off the exploitation of data both domestically and internationally.

For Canada, going along with the American model is the worst of both worlds; we get the surveillance and exploitation, without the economic returns. But the answer for Canada isn't to find ways to capture the returns of unchecked surveillance and data exploitation ourselves.

Rather, Canada should look to implement a data governance framework that restricts predatory practices and enables secondary re-use to deliver benefits for public interest.

As we look for inspiration from peer jurisdictions, Europe has taken the most substantial measures to enact stronger privacy laws. Canada can take inspiration from the EU's Digital Markets Act, which requires gatekeeper platforms to provide meaningful interoperability and data portability tools, and the General Data Protection Regulation (GDPR),[18] which includes the right to data erasure among many others.

In some cases, interoperability requirements are sector-specific, like in Israel's Medical Information Mobilization Law, which gives patients the right to easily transfer their health data to promote the continuity of care, based on standardized data formats.[19]

The EU has also gone further in restricting how personal data can be used — beyond PIPEDA's vague requirements that it be collected for a legitimate purpose. As an example, GDPR provides the right to not be subject to decisions based solely on automated decision-making, and the EU AI Act places limits on what and how data can be used in AI development.[20] A modernized PIPEDA could go much further in prescribing both allowed and prohibited collection of data by private sector actors.

Europe has also led in empowering data protection authorities, with meaningful investigating and auditing powers to monitor for compliance. European data protection authorities can also pursue much more substantial penalties for non-compliance.

While the EU's approach to data protection is far from perfect — it has received its fair share of valid critiques and faced numerous implementation hurdles — it is still far more robust and comprehensive than anything Canada has on the books. The approach is risk-based, rooted in legislation, pursues clear values about how technology should operate, and provides foundational data rights to individuals.

But the EU has not focused exclusively on heavy-handed enforcement.

The EU's 2019 Open Data Directive encourages EU member countries to make public information available for reuse whenever possible, especially research data resulting from publicly funded activities.[21] For protected public sector data, which includes both personal and commercially confidential data, the EU Data Governance Act provides the necessary safeguards to enable reuse.[22]

Among other measures, it defines technical requirements for public sector bodies, establishes rules for data intermediaries, and creates what is effectively a "data altruism" certification scheme for entities that make their data available.

The Act is founded on the recognition that the reuse of all types of data, including protected data, can deliver benefits with appropriate governance.[23]

The U.K.'s 2019 National Data Strategy similarly recognizes data as an asset for innovation[24] — with a mandate to unlock the value of data across the economy by making data usable, accessible and available, while protecting privacy and IP.[25]

More recently, the U.K. Data (Use and Access) Act lays the legislative foundations for mobilizing data.[26]

Stronger Canadian Data Protections

As we have seen in previous chapters of *Foundations of Digital Sovereignty*, governance of the digital realm is about asserting Canadian sovereignty. More assertive data governance will allow Canadians to have better control over how their data is used, and shield them from exploitative forms of collection and targeting.

In creating proper channels for reuse, strong governance creates a structure for Canadians to be the primary beneficiaries of innovation enabled by Canadian data. To achieve this, Canadian data governance legislation must go beyond requiring only consent for the collection of personal data for any "legitimate" purpose.

Data collectors must be obligated to provide users with:

- Egress tools
- Knowledge about how their data is being collected and used
- Meaningful opt-out rights
- The ability to effectively use third-party software or tools
- Rights to have their information deleted or rectified

Updated data governance must include additional requirements for disclosing to users how their data might be used in AI development.

To limit misuse and exploitation, there must be limits on how data can be collected and used. In specific cases, such as with sensitive biometric data, the government should consider more stringent and prescriptive rules. Some data targeting, such as using private data to dynamically set prices, could be banned entirely.

Data collectors should have clear reporting obligations, and privacy regulators should be equipped with strengthened auditing and investigative powers. Legislation could also prescribe specific protections to ensure the privacy and confidentiality of personal information, such as requiring end-to-end encryption from all electronic communications providers.

Data collectors, including public sector bodies, must also be required to provide necessary tools to mobilize data and enable reuse. The legislation should establish and define the principle that reuse of Canadian data should deliver tangible benefits to Canadians.

Data can be used for nefarious purposes as much as socially beneficial ones, and access to data must be conditional on the type of usage proposed and the potential social implications. Clear legal requirements, with vigorous enforcement, is key to creating the kind of public trust that is necessary for unlocking value from Canadian data.

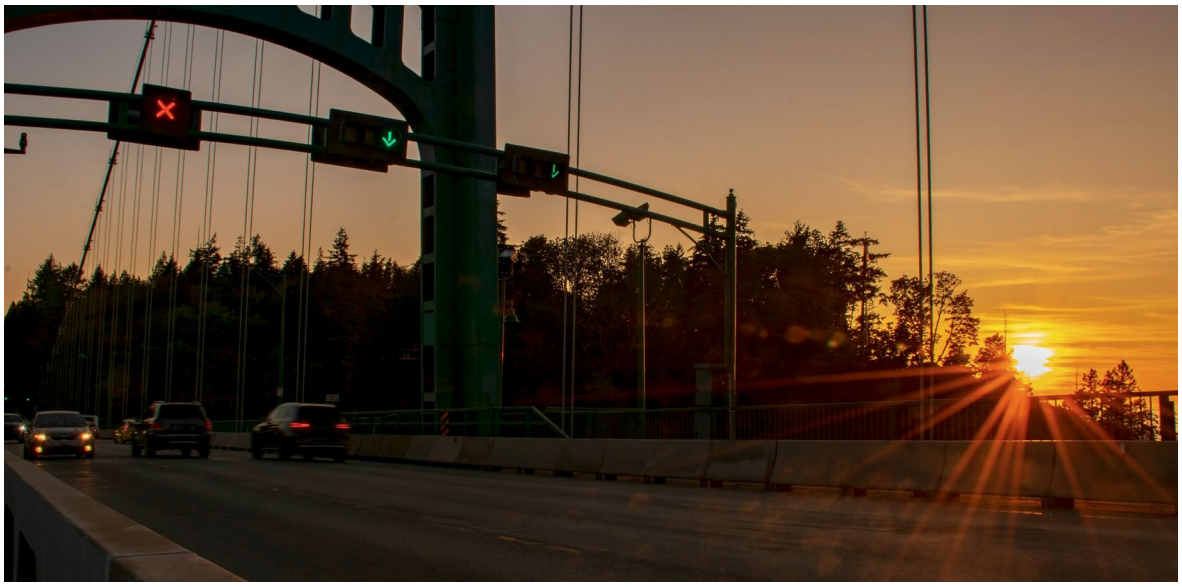
Other Jurisdictions That Do Better

A data trust is a flexible governance model centred around an institution that is authorized to provide stewardship over data, often with the mission of deriving social benefits from data through research and innovation. The data trust makes decisions about who can access and use the data that it collects.

Many other jurisdictions have turned to the data trust model to capture more value from the secondary use of data. As the following examples illustrate, data trusts can be equipped to hold many different types of data, from open public sector data, to sensitive and identifiable health data.

It is no coincidence that Europe also provides a roadmap for building institutions to leverage data for public benefit, given its strong data governance framework. The EU is currently building Common Data Spaces to make data securely available for uses that can deliver benefits for businesses and citizens.[28]

Data spaces will be deployed in key priority areas, including health and agriculture. The European Data Union Strategy committed to scaling up the data spaces, adding defence to the list of priorities.[29] The EU has also announced that it intends to link the data spaces to AI ecosystems.



The European Commission also makes available an open-source middleware platform, called Simpl, to facilitate access and interoperability among the data spaces.[30]

Within the U.K., the Administrative Data Research partnership links together data held by different government bodies.[31] This system enables secure access to newly joined-up and de-identified datasets for research to inform better policy decisions.

Data sets are hosted in a network of trusted research environments, and researchers can apply to access them for any research in the public interest. Other initiatives are underway, like a "British Library for the AI age" to house valuable large-scale data sets for more ambitious AI research,[32] and a National Data Library for improving public sector data access and sharing.[33]

Data trust models are also frequently in use for health system data. The Estonian Biobank is a population-based biobank, currently representing about 20% of Estonia's adult population, that researchers can apply to access securely.[34] In Barcelona, the European Genome-phenome Archive houses and makes available personally identifiable, genetic, phenotypic and clinical data for research.[35]

The Finnish Social and Health Data Permit Authority (or Findata)[36] acts as a trust for data held by various controllers, including public data holders, private service providers and the Kanta Services,[37] and grants permits to access this data for secondary use. Other examples include Israel's Clalit Research Institute, the Danish National Patient Registry, and health data provided by NHS Digital, all of which explicitly aim to deliver benefits to society through health innovation.[38]

Mobilizing Canadian Data for Public Benefit

To mobilize Canadian data for public benefit, Canada should build a national data trust and data exchange platform as a companion to stronger data legislation and regulation.

Canada's national data trust would host, protect, and provide principled access to institutional and proprietary data with the express purpose of promoting the public good and Canadian interests. This would explicitly include projects with an economic benefit to Canada. The data trust would focus primarily on consolidating research data, government data suitable for public use, and open access data of cultural, historical, or community value, making these broadly accessible to Canadian companies, researchers, and institutions.

The core principles governing the data trust would fall into two categories.

On governance, the trust must be oriented toward public benefit. It must require multi-stakeholder involvement in data access decisions, and establish conditions for access depending on the sensitivity of the data.

When companies are using data from the public trust for commercial purposes, IP resulting from that work must be retained in Canada, for the benefit of the Canadian economy.

Strategic and sensitive data categories — defence, health, agriculture, research, and community and Indigenous data — must be prioritized for protection and hosting first.

On architecture, the trust should operate through a centralized model, ensuring data is accessible through a single portal. The government should create tax incentives and funding measures to encourage entities to submit data to the trust. At the same time, the trust should be designed so that companies see real value in participating.

Canada's data resources hold vast potential for creating economic value. Canadian data can also be utilized for research, public health, trade, and defence. Currently, much of this data is being under-utilized because Canadians' primary experience of the data-driven economy is through exploitation.

This exploitation takes increasingly predatory forms — targeted advertising, attention manipulation and algorithmic pricing that uses personal data to manipulate the individual consumer experience.

Alongside strong data governance legislation, the national data trust can position itself as an institution that can safeguard against exploitative behaviour, while allowing companies to engage in commercial activity with new and valuable data sets. When properly de-identified and governed, personal data can ethically serve pro-social ends like optimizing government services, informing public health responses, and enhancing national security without crossing into mass surveillance.

Health

Health data offers one of the clearest opportunities for realizing value from data. Live public health data and national disease databases can direct resources where they are most needed and drive innovation in areas like drug discovery. Canada's data is highly valued globally because of our diverse population but even more so because of the longitudinal nature of health data in the country, meaning that most people have health data from when they are born to when they die, creating extremely valuable data sets at the population level.

The challenge is that Canadian health data, while relatively well protected, is highly fragmented across provincial and territorial systems and increasingly hosted on foreign-owned infrastructure.[39] As we will see in future chapters of *Foundations of Digital Sovereignty,* there are real risks to data security that come with foreign-controlled cloud infrastructure.

The reliance on foreign-controlled infrastructure also gives rise to the potential for predatory arrangements where data service providers try to leverage the offer of advanced AI and other tools to institutions in exchange for access to their data. The often dubious promise of enhanced productivity offered to cash-strapped institutions is an easy sell to extract truly valuable underlying assets from them. Health data is also inseparable from national security: mobilized responsibly it strengthens emergency response and social cohesion, but through ungoverned partnerships it becomes a vulnerability that adversaries can exploit and that erodes government capacity when it is needed most.

A Canadian national data trust can act as a sovereign repository, while deploying high-value health data for public benefit uses.

Defence

Defence presents a similarly double-edged picture. Better data flows and AI-assisted decision-making can strengthen Canada's security posture, but consolidating sensitive defence data introduces risks of privacy violations and surveillance overreach.

Relying on foreign contractors like Palantir and Anduril — whose systems are associated with mass surveillance and ethically questionable targeting — poses direct data sovereignty risks.

Simply replacing them with domestic equivalents doesn't resolve the problem if proprietary data is still misused in the name of national security. Canada's defence community is actively working through where ethical concerns must override the potential advantages of algorithmic tools.[40]

Publicly Funded Research

Research data is an additional underutilized asset. Canadian institutions are world class, and they produce vast amounts of data across disciplines with immediate and long-term value.

Better infrastructure to organize, share, and analyze these datasets — potentially using AI to surface cross-disciplinary patterns — could provide major strategic advantages, advance human knowledge tremendously, and support trustworthy national and international data marketplaces.

This potential is already being constrained, however, by academic publishers who own vast swaths of academic copyright material while also owning the platforms through which to manage and access catalogues, asserting control over institutional metadata and restricting what institutions are able to do with their own data to protect commercial interests.

This is another area where a national data trust could act as a centralized repository and co-ordinating institution.

Because the national data trust infrastructure will serve as the foundation for other systems and emerging projects, it must be developed thoughtfully and sustainably.

A pilot phase would be valuable in testing key elements — health data is a natural candidate given the urgency of need — but any pilot must be national in scope from the outset. A regionally limited pilot risks entrenching systems that later face serious interprovincial interoperability challenges, undermining the very consolidation the trust is meant to achieve.

Equally, the governance and development process must be broadly collaborative, ensuring no province, class of institution, or community is excluded. Trust-building is not incidental to this project — it is foundational to it.

Canada need not start from scratch. Existing projects like the Borealis Canadian Dataverse Repository, the Statistics Canada data portal, the CAMH BrainHealth Databank, the Canadian Research Data Centre Network, and the Canada-based Internet Archive all offer lessons in governance and technical design that should inform the national trust's development.[41]

These projects demonstrate both what is possible and where the gaps in Canada's current data infrastructure are most acute. A national data trust would not replace these efforts — it would give them the sovereign, governed, and strategically oriented home they currently lack.

Conclusion

Canada stands at a crossroads.

Our data wealth is vast and its strategic potential enormous, but without action, wealth will continue to be extracted, exploited, and turned into value that accrues elsewhere.

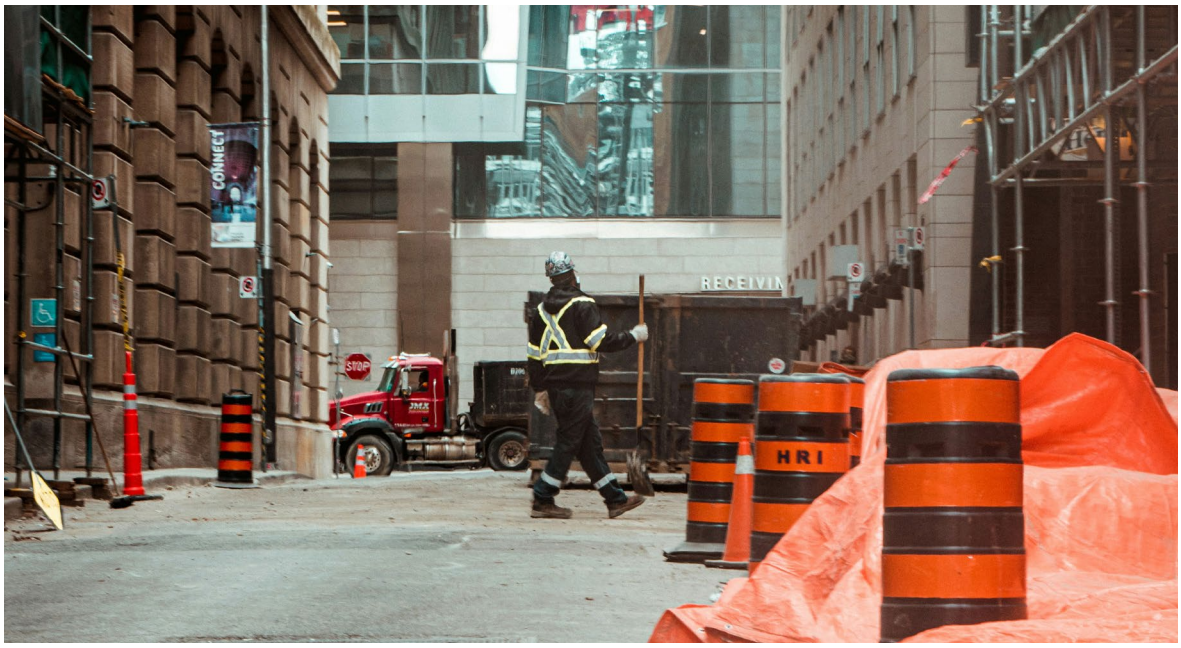
Currently, we are stuck in a bad dynamic where consumers feel distrustful of data-driven technologies, which in turn hinders Canada from innovating and reaping the prosperity of the data-driven economy.

The legislative gaps diagnosed in this paper reflect a failure to reckon seriously with data as a foundational national asset.

Closing those gaps through comprehensive data legislation, and building our infrastructure to govern and mobilize Canadian data through a national data trust, would represent a true shift. Ultimately, Canada must embrace a role in the intangibles economy as a sovereign actor with the tools to protect our citizens, support our institutions, and compete on our own terms.

The window to act is narrowing.

Every year without a coherent data strategy is a year where Canadian data is scattered, unprotected, and quietly working against Canadian interests.



Solutions

Canada needs to take a two-step approach to governing our data. This approach must build trust and social licence by protecting citizens from exploitation, while simultaneously unlocking proprietary Canadian data for research, innovation and commercialization.

1 The Government of Canada must pass data governance legislation that establishes guardrails for the collection of personal data for any "legitimate" purpose. Data collectors must be obligated to provide users with egress tools, knowledge about how their data is being collected and used, meaningful opt-out rights, the ability to effectively use third-party software or tools, and rights to have their information deleted or rectified. Meaningful data governance must include meaningful power for Canadian privacy regulators to enforce these obligations. Updated data governance must include additional requirements for disclosing to users how their data might be used in AI development.

2 Canada must establish a national data trust and data exchange platform to host, protect and provide access to institutional and proprietary data. The express purpose must be to promote the public good and Canadian interests, explicitly including projects with an economic benefit to Canada.

References

1 Meta, "Meta Reports Fourth Quarter and Full Year 2025 Results," January 28, 2026, https://investor.atmeta.com/investor-news/press-release-details/2026/Meta-Reports-Fourth-Quarter-and-Full-Year-2025-Results/default.aspx.

2 Statistics Canada, "The value of data in Canada: Experimental estimates," Government of Canada, July 10, 2019, https://www150.statcan.gc.ca/n1/pub/13-605-x/2019001/article/00009-eng.htm.

3 Dan Ciuriak, "Enterprise Value and the Value of Data," Centre for International Governance Innovation, CIGI Papers, no. 327 (2025), https://www.cigionline.org/publications/enterprise-value-and-the-value-of-data/.

4 Graham Dobbs, "The Digital Dividend: The Economic Potential of Canada's Data Sovereignty," Signal49 Research, March 17, 2026, https://www.signal49.ca/insights/the-digital-dividend-the-economic-potential-of-canadas-data-sovereignty/.

5 Privacy Commissioner of Canada, "Statement by the Privacy Commissioner of Canada to the Standing Committee on Access to Information, Privacy and Ethics on its study of artificial intelligence," February 2, 2026, https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2026/parl_260202/.

6 Privacy Act, R.S.C., 1985, c. P-2, https://laws-lois.justice.gc.ca/eng/ACTS/P-21/index.html.

7 PIPEDA, S.C., 2000, c. 5, https://laws-lois.justice.gc.ca/eng/acts/p-8.6/.

8 Tamara Nielsen, Ryan Black and Tyson Gratton, "And then it grew teeth: Canada's privacy law gets enforcement-laden overhaul," DLA Piper, November 17, 2020, https://www.dlapiper.com/en-ca/insights/publications/2020/11/new-canadian-federal-privacy-statute.

9 Office of the Privacy Commissioner of Canada, "PIPEDA Fair Information Principle 3 – Consent," accessed April 16, 2026, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_consent/.

10 Office of the Privacy Commissioner of Canada, "PIPEDA Fair Information Principle 2 – Identifying Purposes," accessed April 16, 2026, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_purposes/%5C.

11 Teresa Scassa, "Replacing Canada's 20-Year-Old Data Protection Law," Centre for International Governance Innovation, December 23, 2020, https://www.cigionline.org/articles/replacing-canadas-20-year-old-data-protection-law/.

12 Lisa Austin, "Who decides? Consent, meaningful choices, and accountability," Schwartz Reisman Institute for Technology and Society, December 22, 2020, https://srinstitute.utoronto.ca/news/austin-consent-meaningful-choice-accountability.

13 Scassa, "Replacing Canada's 20-Year-Old Data Protection Law;" Amanda Cutinha and Christopher Parsons, "Mobility Data and Canadian Privacy Law Explained," Citizen Lab, November 22, 2022, https://citizenlab.ca/research/a-critical-analysis-of-the-collection-of-de-identified-mobility-data/mobility-data-and-canadian-privacy-law-explained/.

14 Teresa Scassa, "How Facebook's Poor Privacy Practices Shed Light on PIPEDA's Shortcomings," Centre for International Governance Innovation, February 13, 2020, https://www.cigionline.org/articles/how-facebooks-poor-privacy-practices-shed-light-pipedas-shortcomings/.

15 Cathy Jares, "Anonymization and De-Identification: A Comparison of PIPEDA and Bill C-27," Aird Berlis, September 25, 2023, https://www.airdberlis.com/insights/publications/publication/anonymization-and-de-identification-a-comparison-of-pipeda-and-bill-c-27.

16 Cutinha and Parsons, "Mobility Data and Canadian Privacy Law."

17 Chantal Bernier and Rohinton P. Medhora, "Despite Best Intentions, Bill C-11 Misses the Mark on Fostering Innovation in Canada," Centre for International Governance Innovation, February 12, 2021, https://www.cigionline.org/articles/despite-best-intentions-bill-c-11-misses-mark-fostering-innovation-canada/.

18 European Parliament and Council of the European Union, Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] Official Journal of the European Union L119/1, https://gdpr-info.eu/.

19 European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Official Journal of the European Union L 2024/1689, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

20 European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), Official Journal of the European Union L 2024/1689. ; European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), art.5, Official Journal of the European Union L 2024/1689, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-:32024R1689.

21 European Commission, "European legislation on open data," last modified November 19, 2025, https://digital-strategy.ec.europa.eu/en/policies/legislation-open-data.

22 European Commission, "Data Governance Act explained," accessed April 16, 2026, https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained.

23 European Commission, "European Data Governance Act," last modified October 10, 2024, https://digital-strategy.ec.europa.eu/en/policies/data-governance-act.

24 Department for Digital, Culture, Media & Sport, "National Data Strategy," Gov.UK, last modified December 9, 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy.

25 Department for Science, Innovation & Technology, and Department for Digital, Culture, Media & Sport, "National Data Strategy Mission 1 Policy Framework: Unlocking the value of data across the economy," Gov.UK, November 24, 2021, https://www.gov.uk/government/publications/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy.

26 Data (Use and Access) Act, UK Public General Acts, 2025 c. 18, https://www.legislation.gov.uk/ukpga/2025/18/contents.

27 Ministry of Social Affairs and Health (Finland), "Secondary use of health and social data," accessed April 16, 2026, https://stm.fi/en/secondary-use-of-health-and-social-data.

28 European Commission, "Common European data spaces," last modified November 19, 2025, https://digital-strategy.ec.europa.eu/en/policies/data-spaces.

29 European Commission, "European Data Union Strategy," last modified March 20, 2026, https://digital-strategy.ec.europa.eu/en/policies/data-union.

30 European Commission, "Simpl: Cloud-to-edge federations empowering EU data spaces," last modified October 11, 2024, https://digital-strategy.ec.europa.eu/en/policies/simpl.

31 UK Research and Innovation, "Administrative Data Research UK (ADR UK)," last modified February 5, 2026, https://www.ukri.org/what-we-do/browse-our-areas-of-investment-and-support/administrative-data-research-uk-adr-uk/.

32 University of Bristol, "University of Bristol to develop multimillion-pound new 'British Library' for the AI age," November 21, 2025, https://www.bristol.ac.uk/news/2025/november/university-of-bristol-to-develop-new-british-library-for-the-ai-age.html.

33 Department for Science, Innovation & Technology, "National Data Library: progress update, January 2026," Gov.UK, January 26, 2026, https://www.gov.uk/government/publications/national-data-library-progress-update-january-2026/national-data-library-progress-update-january-2026.

34 University of Tartu, "Estonian Biobank," accessed April 16, 2026, https://genomics.ut.ee/en/content/estonian-biobank.

35 European Genome-Phenome Archive, "About," accessed April 16, 2026, https://ega-archive.org/about/ega/.

36 Finnish Social and Health Data Permit Authority, "Front page," accessed April 16, 2026, https://findata.fi/en/.

37 Finland's Kanta Services are a set of nationwide IT solutions used by both public and private healthcare providers: Kanta, "What are the Kanta Services?," last modified February 5, 2026, https://www.kanta.fi/en/what-are-kanta-services.

38 Israel Healthcare Foundation, "Research and Innovation," accessed April 16, 2026, https://israelhealthcarefoundation.org/research-and-innovation/; Danish Health Data Authority, "National health registers," accessed April 16, 2026, https://english.sundhedsdatastyrelsen.dk/health-data-and-registers/national-health-registers; NHS England, "Data," accessed April 16, 2026, https://digital.nhs.uk/data.

39 Michael Geist, Mari Teitelbaum and Kumanan Wilson, "Ensuring the sovereignty and security of Canadian health data," Canadian Medical Association Journal 197, no. 26 (2025), https://doi.org/10.1503/cmaj.250488.

40 The complexities of integrating AI into already well-established military practices is explored in depth in a forthcoming paper on DND/CAF integration of AI into existing cognitive hierarchy and decision-making frameworks: Colonel Adam Moore and Matthew da Mota, "Navigation by Sextant & Astrocompass: A CAF Approach for AI Adoption," Canadian Military Journal, forthcoming Spring/Summer 2026.

41 Borealis, "The Canadian Dataverse Repository," accessed April 16, 2026, https://borealisdata.ca/; Statistics Canada, "Open data, statistics and archives," last modified February 3, 2022, https://www.canada.ca/en/services/science/open-data.html; Centre for Addiction and Mental Health (CAMH), "BrainHealth Databank," accessed April 16, 2026, https://www.camh.ca/en/science-and-research/discovery-fund/brainhealth-databank; Canadian Research Data Centre Network, "Home," accessed April 16, 2026, https://crdcn.ca/; Internet Archive, "About," accessed April 16, 2026, https://archive.org/about/.