Data & Policy (2026), 8: e37
doi:10.1017/dap.2026.10085

CAMBRIDGE UNIVERSITY PRESS

COMMENTARY

Middle powers in the platform economy: Digital sovereignty after the data pivot

Thierry Warin

International Business, HEC Montreal, Canada
Email: thierry.warin@hec.ca

Received: 12 May 2026 UTC; **Revised:** 17 June 2026 UTC; **Accepted:** 26 June 2026 UTC

Keywords: digital sovereignty; middle powers; platform economy; state as a platform

Abstract

This article examines the future of the world economy from the standpoint of middle powers, with particular attention to Canada in the wake of Prime Minister Mark Carney's renewed emphasis on middle-power coordination. It argues that the central economic transformation is not simply digitization, but a deeper pivot from the production of goods and knowledge toward the valuation of data generated through those production processes. Agriculture, manufacturing, health, education, logistics, and public administration are increasingly organized around data capture, platform intermediation, and AI-enabled recombination. This shift intensifies economies of scale, network effects, and economies of scope, thereby concentrating economic power in a small group of multinational technology firms. For middle powers, the resulting challenge is not to reject global platforms, but to avoid operational dependency on them. The article advances digital sovereignty as a framework based on control, interoperability, public-interest data governance, sovereign compute, and contestable digital markets. It concludes that middle powers must develop the state as a platform: a provider of trusted digital foundations that can sustain innovation, democratic accountability, and strategic autonomy in an increasingly platformized world economy.

Policy Significance Statement

Middle powers face a structural policy problem: data generated across agriculture, manufacturing, health, education, logistics, and public administration is increasingly captured and monetized through foreign-controlled platforms. This article argues that digital sovereignty should not be understood as technological isolation, but as the capacity to govern data, compute, interoperability, procurement, and platform dependency under public law. For policymakers, the central implication is that digital infrastructure has become economic infrastructure. High-capacity middle powers can build public digital foundations, support sovereign compute, require data portability, and prevent lock-in. Capacity-constrained middle powers can pursue pooled procurement, shared cloud-certification standards, regional data-governance arrangements, and coalition-based access to compute. Across these variants, coordination with other middle powers remains necessary to preserve competition and democratic accountability. The article offers a policy vocabulary for designing open, interoperable, and rights-preserving state platforms for contemporary economic governance, before platform dependency hardens into permanent constraint.

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/dap.2026.10085 Published online by Cambridge University Press

1. Introduction

The renewed language of middle powers is not merely diplomatic theatre. It is a symptom of a deeper economic reordering. When Mark Carney argued at the World Economic Forum that middle powers are not powerless in an era of great-power rivalry, he was speaking from a Canadian position, but the proposition travels well beyond Canada (Carney, 2026). The same question now confronts a wide family of states: how can countries preserve economic agency when the world economy is being reorganized around data, compute, and platforms? This question concerns Canada, Australia, South Korea, Japan, Singapore, the Netherlands, Germany, Brazil, India, Indonesia, Mexico, South Africa, and many others. Their histories, institutions, and geopolitical positions differ. Yet they share a common predicament. They are large enough to matter, but not large enough to dictate the architecture of the global digital economy alone.

This article therefore uses Canada as the motivating case and the European Union as the closest institutional comparator, rather than as evidence that all middle powers possess the same implementation capacity. The framework is differentiated. High-capacity middle powers with fiscal space, regulatory competence, public-sector technical expertise, energy infrastructure, and political alignment can pursue national or regional public digital infrastructure, trusted cloud procurement, and public-interest compute. Capacity-constrained middle powers may need more modular instruments: sectoral data intermediaries, shared cloud-certification rules, pooled procurement, interoperability clauses in trade and regulatory agreements, and participation in regional digital public infrastructure. The common predicament is platform dependency; the feasible response varies with state capacity, market scale, geopolitical exposure, and domestic political alignment.

The traditional vocabulary of economic strategy is still necessary, but it is no longer sufficient. States still need food security, energy systems, ports, railways, hospitals, universities, financial institutions, industrial capacity, and defence capabilities. Yet the old separation between the physical economy and the digital economy has become increasingly misleading. A farm is no longer only land, labour, seeds, machinery, and weather. It is also soil analytics, satellite imagery, climate modelling, logistics software, insurance data, commodity forecasting, and platform-mediated market access. A car is no longer only steel, glass, rubber, batteries, and engineering. It is a connected data environment shaped by sensors, software updates, mapping systems, entertainment services, predictive maintenance, usage-based insurance, and eventually autonomous-driving models. A hospital is not only a site of care. It is also a repository of longitudinal clinical data, diagnostic images, genomic information, administrative records, and AI-training potential. A university does not merely produce knowledge. It also generates research data, citation graphs, learning analytics, administrative data, and digital traces that can be organized, measured, and monetized.

The decisive shift is therefore not that the economy has stopped producing things or knowledge. It is that a growing share of economic value is now captured from the data generated in the production of things and knowledge. Production remains real, material, and labour-intensive. But the valuation layer increasingly migrates upward, toward firms that control data, interfaces, cloud infrastructure, models, and the platforms through which producers reach users, suppliers, regulators, and one another. This is why the data economy cannot be treated as a sector beside agriculture, manufacturing, finance, health, education, or energy. It is becoming the organizing layer across all of them.

2. From production to data valuation

This is the central paradigm change. Industrial capitalism was organized around control of land, labour, machinery, energy, capital, and logistics. Knowledge capitalism added patents, brands, software, research systems, human capital, and intangible investment. Platform capitalism reorganizes these assets around continuous data capture and the ability to recombine data across domains (Srnicek, 2017). Haskel and Westlake (2018) show how intangible assets alter investment, scalability, spillovers, and inequality. The OECD (2022) similarly treats data not as a marginal input but as an asset that shapes firm productivity,

https://doi.org/10.1017/dap.2026.10085 Published online by Cambridge University Press

business models, and market structure. Data is not valuable merely because it exists. It becomes valuable when it can be collected, cleaned, connected, secured, interpreted, and used to redesign decisions at scale.

This explains why economies of scale, network effects, and economies of scope are so central. Scale matters because larger systems collect more observations and spread infrastructure costs across more users. Network effects matter because additional users can make a platform more valuable to other users. Scope matters because data collected in one field can be reused in another. Search data improves advertising. Commerce data improves logistics and credit scoring. Mobility data improves mapping. Cloud usage data improves infrastructure planning. Device data improves consumer profiling. Health data improves diagnostics and insurance models. Education data improves assessment systems and labour-market prediction. These reinforcing dynamics are not incidental. They are intrinsic to platform economics (Rochet and Tirole, 2003; Parker et al., 2016).

The result is a new form of asymmetry. In the nineteenth century, many countries worried that railways, ports, and mines would be owned by foreign capital. In the twentieth century, they worried about oil companies, banks, armaments firms, and global manufacturers. In the twenty-first century, the deeper vulnerability is that the informational layer of the whole economy may be organized by a small number of corporations headquartered elsewhere. This is not simply "Big Tech" in the everyday sense of social media. It is cloud infrastructure, operating systems, app stores, digital identity, payment rails, advertising exchanges, productivity software, cybersecurity systems, artificial intelligence models, developer ecosystems, and the application programming interfaces through which firms and citizens increasingly access economic life (Van Dijck et al., 2018).

UNCTAD (2021) captures the scale of the imbalance. The United States and China account for about 90 percent of the market capitalization of the world's largest digital platforms, while the leading global platforms have been expanding across the entire data value chain. This is not only a competition problem. It is a sovereignty problem. It affects who owns the interface between producers and users, who sets technical standards, who determines the cost of participation, who sees the data, who trains the models, and who can convert one market advantage into another.

The cloud market illustrates the point. Synergy Research Group estimated that enterprise spending on cloud infrastructure services reached about $129 billion in the first quarter of 2026, with Amazon, Microsoft, and Google holding worldwide market shares of 28 percent, 21 percent, and 14 percent, respectively. In public IaaS and PaaS, the top three accounted for 67 percent of the market (Synergy Research Group, 2026). These figures matter because the cloud is not merely another corporate service. It is the infrastructure on which firms, universities, hospitals, public agencies, start-ups, and research laboratories increasingly build their operations. Once an organization's data pipelines, security architecture, AI tools, software development practices, and internal workflows are embedded in one cloud ecosystem, exit becomes costly. Lock-in then becomes a structural condition rather than a contractual inconvenience.

Artificial intelligence deepens the problem. AI is often described as compute-constrained, and this is partly true. Chips, electricity, cooling systems, data centres, and capital expenditure now shape the macroeconomics of digital transformation. The International Energy Agency estimated that data centres consumed about 415 TWh of electricity in 2024, or roughly 1.5 percent of global electricity consumption, and projected that this could more than double to about 945 TWh by 2030 (International Energy Agency, 2025). But compute is not the whole story. Compute is the furnace; data is the ore. Without high-quality, legally usable, domain-specific data, compute produces little more than expensive statistical machinery. The strategic advantage belongs to those who control the full stack: data, compute, energy, models, standards, procurement, rights, and markets.

Sovereign compute should therefore be understood as a portfolio rather than a single asset. At one end, it may involve direct public or publicly supported investment in data centres, high-performance computing, and AI infrastructure for research, public administration, health, security, and industrial policy. At another, it may involve trusted cloud arrangements with private hyperscalers, subject to enforceable rules on data location, encryption, auditability, portability, security certification, and continuity of public services. It may also include chip and GPU supply-chain diversification, coordinated energy planning,

https://doi.org/10.1017/dap.2026.10085 Published online by Cambridge University Press

public procurement of compute for universities and start-ups, and pooled purchasing arrangements among allied or peer states. These strategies are not equivalent. National data-centre investment can increase autonomy, but it is capital-intensive, energy-intensive, and technologically perishable. Public cloud alternatives can reduce dependency, but only if they achieve sufficient scale and reliability. Trusted procurement can be more efficient, but it may leave the deeper architecture of cloud and AI development in foreign hands. The objective for middle powers is not complete self-sufficiency in compute. It is sufficient operational capacity to avoid coercive dependence, preserve public-service continuity, and negotiate with private and foreign providers from a position of credible exit.

3. Digital sovereignty between control and interoperability

For middle powers, this creates a strategic paradox. They cannot replicate every hyperscaler, every AI laboratory, every semiconductor supply chain, every operating system, and every global platform. Autarky is not sovereignty. A closed national digital economy would be poorer, less innovative, and less resilient. Yet dependency is not sovereignty either. If public agencies, firms, researchers, and citizens depend on external platforms whose standards, prices, data practices, model updates, moderation rules, procurement conditions, and security architectures are outside domestic control, sovereignty becomes largely ceremonial. It may remain intact in constitutional language, but not in operational capacity.

This is where digital sovereignty must be defined with precision. It should not mean that every dataset must be stored within national borders. It should not mean nationalization of the digital economy. Nor should it be used as a rhetorical cover for protectionism or surveillance. Digital sovereignty means that a political community retains the practical capacity to set enforceable rules over the collection, movement, storage, processing, monetization, and deletion of data; to secure critical digital infrastructure; to maintain public-interest digital capabilities; to ensure that citizens and firms can exit dominant systems; and to participate in global digital markets without accepting subordination as the price of access. The concept is contested, but its core concerns are authority, control, autonomy, and legitimacy in digital environments (Couture and Toupin, 2019; Floridi, 2020; Pohle and Thiel, 2020).

The crucial distinction is between control and closure. Control does not require isolation. Interoperability does not require surrender. Control without interoperability becomes stagnation. Interoperability without control becomes dependency. The strategic task for a middle power is to design both together. This means data portability, open standards, audit rights, secure APIs, public-interest data access, privacy-preserving analytics, procurement rules that prevent lock-in, competition policy, cybersecurity requirements, and public digital infrastructure. The OECD's work on data access and sharing is useful because it avoids the false binary between open data and closed data. Data governance can involve internal use, restricted sharing, conditional access, trusted intermediaries, and open access, depending on rights, risks, and public purposes (OECD, 2019).

The European Union's Digital Markets Act offers one model of how public authority can respond to platform power. It identifies large digital gatekeepers and imposes obligations intended to make digital markets more contestable. The European Commission currently lists gatekeepers including Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, and Booking, across core platform services such as search, app stores, operating systems, advertising, social networks, messaging, and online intermediation (European Commission, 2023). The relevance for middle powers is not that every state should copy the EU's institutional design. The lesson is broader: digital market power must be governed before it becomes constitutional power by other means. Once a platform becomes the infrastructure of everyday economic life, correction after the fact becomes slow, expensive, and politically fragile.

The state-as-platform argument differs from existing arrangements in its point of intervention. The Digital Markets Act disciplines large gatekeepers after platform power has already become structurally important. OECD data-access work clarifies how data can be shared, restricted, or governed across different risk environments. Both are necessary, but neither is sufficient. A state-as-platform strategy asks a prior institutional question: what public digital foundations must exist before firms, citizens, researchers, and agencies enter negotiations with dominant platforms? The first-order policy moves

https://doi.org/10.1017/dap.2026.10085 Published online by Cambridge University Press

are therefore not only competition remedies or general data-sharing principles. They include public procurement rules that prohibit lock-in, mandatory exit clauses in cloud contracts, interoperable digital identity and payments systems, audit rights for critical algorithms and cloud services, trusted data intermediaries in strategic sectors, public-interest compute for research and small firms, open technical standards, and cross-border procurement coalitions. Success would not mean replacing global platforms with national replicas. It would mean that public agencies, universities, hospitals, municipalities, and domestic firms can use global platforms without becoming technically or contractually trapped by them.

4. The state as a platform

The more constructive answer is the state as a platform. The phrase is easily misunderstood. It does not mean that the state should behave like a private platform corporation. It means that the state should provide foundational digital capabilities on which citizens, firms, researchers, civil society organizations, municipalities, and public agencies can build. O'Reilly (2011) argued that government can become a platform when it offers reusable infrastructure, open interfaces, shared services, and public data resources rather than only finished bureaucratic products. In contemporary policy language, this idea overlaps with digital public infrastructure. The OECD (2024) defines digital public infrastructure as secure, interoperable shared digital systems that support inclusive access to public and private services, including digital identity, payments, data sharing, digital post, and core government registries.

Recent work on digital and data-driven transformations in governance emphasizes that data infrastructures do not merely improve administrative efficiency; they reshape participation, organizational relations, public services, and the institutional conditions under which governments exercise authority (Giest et al., 2025).

For middle powers, the state-as-platform idea is not administrative modernization alone. It is economic strategy. A country that lacks foundational digital infrastructure will bargain with platforms one agency, one firm, one university, and one municipality at a time. That country will be structurally weak. A country that builds interoperable public digital infrastructure can aggregate demand, set standards, reduce duplication, lower entry barriers for domestic firms, protect citizens' rights, and negotiate with global platforms from a stronger position. This is not anti-market. It is the public construction of the conditions under which markets remain contestable.

Canadian debates on digital sovereignty have already shown that platform dependence is not only an industrial-policy issue but also a problem of privacy, public trust, cross-border data exposure, and democratic vulnerability (Stevens et al., 2020).

The sectoral implications are substantial. In agriculture, middle powers should prevent farm data from being monopolized by equipment manufacturers, input suppliers, or logistics platforms. Farmers should be able to benefit from pooled agronomic data without surrendering permanent control over it. In manufacturing, firms should not be forced into proprietary industrial systems that make data portability impossible. If public funds support advanced manufacturing, procurement conditions should require interoperability, data access rights, and transparent governance. In health, public data should be available for legitimate research and innovation under strict privacy, consent, and security conditions, but it should not become a private enclosure of public medical knowledge. In education, learning analytics should improve teaching and public understanding rather than create behavioural markets around students. In energy, grid data and consumption data should support decarbonization, resilience, and planning without producing new forms of private surveillance.

The economic logic is simple but often ignored. If data has increasing returns to scope, then fragmented public data is wasted capital. If private platforms capture sectoral data exclusively, domestic producers become tenants in someone else's informational economy. A country may still produce the food, manufacture the vehicles, train the engineers, treat the patients, and educate the students. Yet the most valuable layer of prediction, optimization, pricing, and market access may be captured elsewhere. This is how dependency develops quietly. It does not always appear as a lost factory or a closed mine. It appears as a gradual migration of economic intelligence to external platforms.

https://doi.org/10.1017/dap.2026.10085 Published online by Cambridge University Press

Working with technology giants is therefore unavoidable, but the form of cooperation matters. The goal should not be hostility toward large technology companies. Hyperscalers possess capabilities that many states and domestic firms need: cloud infrastructure, cybersecurity expertise, AI tooling, global reliability, and capital-intensive engineering. The problem is asymmetric bargaining. A middle power that negotiates separately through each ministry, hospital, university, and start-up will lose leverage. A middle power that coordinates procurement, defines technical standards, requires portability, insists on auditability, and cooperates with peer countries can transform dependency into disciplined interdependence.

The difference between dependency and interdependence is exit. Interdependence can be strategically acceptable when exit remains possible. Dependency becomes dangerous when exit is technically, financially, or administratively impractical. The test of digital sovereignty is therefore not whether a public agency uses a foreign cloud provider or whether a domestic firm sells through a global platform. The test is whether the agency or firm can know where sensitive data is stored, understand how it is processed, audit compliance, migrate workloads if required, preserve public-service continuity, and avoid being trapped by proprietary formats, unilateral price changes, or opaque model updates. Control is meaningful only when it is operational.

Competition policy must also change. Traditional antitrust tools remain important, but platform markets require attention to data concentration, default settings, self-preferencing, app-store rules, cloud credits, bundling, killer acquisitions, advertising opacity, and the cross-market leverage of data. Khan's (2017) analysis of Amazon remains important because it shows why price-centred antitrust may miss structural power in platform markets. A digital service may appear cheap or even free, while the underlying harm appears elsewhere: reduced innovation, weakened small firms, degraded privacy, reduced bargaining power, dependency of public institutions, manipulation of information environments, and erosion of domestic productive capacity.

A single middle power may struggle to discipline global platforms. A coalition of middle powers is harder to ignore. This is where the old idea of middle-power diplomacy needs to be adapted to the platform age. The classic literature often described middle powers as states that seek multilateral solutions, coalition-building, and rule-based order (Cooper et al., 1993; Jordaan, 2003). That tradition remains useful, but the domain has changed. Middle-power cooperation should now include AI safety and evaluation, sovereign public compute, trusted cloud standards, cross-border data governance, privacy-preserving research infrastructures, digital identity interoperability, public procurement rules, competition remedies, and technical standards for portability and auditability.

At the municipal scale, the smart city debate shows that platformization is not simply a matter of private technology adoption; it is also a transformation of public administration, procurement, contracting, and the capacity of governments to govern data-intensive urban systems (Zwick and Spicer, 2024).

Such coalitions do not require one grand alliance. They require variable geometry: different coalitions for different problems. A country may cooperate with one group on AI safety, another on cloud procurement, another on semiconductor resilience, another on health-data governance, and another on platform competition. The objective is not ideological purity. It is bargaining capacity. Middle powers need enough collective scale to shape standards before standards shape them, especially in regulatory domains where great powers retain disproportionate agenda-setting capacity (Drezner, 2007).

A neorealist objection must be taken seriously here. Middle powers do not operate outside anarchy, nor do they automatically prefer cooperation to competition (Waltz, 1979). Where compute capacity, standards, data access, AI models, cloud infrastructure, and technical certification generate first-mover advantages, states may worry less about absolute collective gains than about relative gains (Grieco, 1988; Snidal, 1991). A middle power may therefore seek to attract data-centre investment before its peers, subsidize national AI champions, localize strategic data, or design procurement rules that favour domestic firms. This behaviour is not irrational. It reflects the positional logic of a digital economy in which standards and infrastructures can harden early and distribute future bargaining power unevenly. Yet this same neorealist logic also explains why selective cooperation may be necessary. An isolated middle power competing alone against great powers and global platform firms is likely to exchange autonomy for access. A coalition of middle powers can be understood not only as liberal institutionalism, but also as a

https://doi.org/10.1017/dap.2026.10085 Published online by Cambridge University Press

form of balancing (Waltz, 1979; Keohane, 1984; Grieco, 1988): a way to increase bargaining capacity, preserve exit options, prevent standards from being set externally, and reduce dependence on infrastructures controlled elsewhere. The realistic conclusion is therefore not that middle powers will cooperate across all domains. They will compete in some areas and coordinate in others. The strategic task is to identify where rivalry is unavoidable and where shared rules are the condition of avoiding deeper subordination.

5. The democratic limits of digital sovereignty

Yet the state-as-platform strategy also carries risks. Public digital infrastructure can become a tool of inclusion, innovation, and sovereignty. It can also become a surveillance architecture (Zuboff, 2019). Digital identity, payments, registries, health records, education data, and public-service portals are powerful precisely because they touch daily life. If they are designed without rights, transparency, oversight, contestability, and cybersecurity, they can centralize vulnerability and normalize monitoring. Digital sovereignty must therefore be constitutional as well as operational. It must include due process, privacy, independent oversight, public accountability, and meaningful remedies. Otherwise, a state may escape private platform dependency only to construct a public platform of excessive administrative power.

This is why the concept of control must be bounded. A democratic state should not collect all data merely because it can. It should not make participation in public life dependent on opaque systems. It should not treat citizens as data sources first and rights-bearing persons second. The purpose of public digital infrastructure is to increase collective capability while preserving individual autonomy. The relevant standard is not maximum data extraction. It is legitimate, proportional, secure, and purpose-bound data use.

The future world economy is likely to be more fragmented than the globalization of the 1990s, more strategic than the liberalization agenda of the early 2000s, and more data-intensive than earlier industrial policy imagined. Great powers will use supply chains, chips, cloud services, standards, finance, export controls, AI models, and platforms as instruments of leverage, a pattern that resembles what Farrell and Newman (2019) describe as weaponized interdependence. The old assumption that economic integration automatically produces mutual benefit is no longer credible. But the opposite assumption, that each country can retreat into a digital fortress, is equally false. Middle powers need a third position: open enough to innovate, sovereign enough to negotiate, and coordinated enough to matter.

This requires a shift in how governments understand economic policy. Data should be treated as seriously as energy, food, capital, infrastructure, and defence. Not because data replaces these domains, but because it increasingly reorganizes their value. A country may produce food, but if agronomic data, logistics intelligence, commodity forecasting, and retail platforms are controlled elsewhere, part of the value chain has already moved. A country may manufacture vehicles, but if vehicle data, operating systems, charging networks, insurance analytics, and autonomous-driving stacks are controlled elsewhere, manufacturing becomes a lower-margin component of a larger platform economy. A country may produce knowledge, but if research infrastructure, educational platforms, scientific databases, and AI tools are controlled elsewhere, intellectual sovereignty erodes quietly.

6. Conclusion: sovereignty without closure

The answer is not nostalgia for an economy of things. It is the construction of an economy in which the data generated by things and knowledge can be governed, shared, protected, and valued in the public interest. The middle power that succeeds will not be the one that rejects platforms. It will be the one that understands platform power well enough to build public counterweights, negotiate disciplined partnerships, and preserve contestability. The state as a platform is not a slogan for bureaucratic digitization. It is a strategy for ensuring that public authority, democratic rights, and domestic productive capacity are not reduced to permissions granted by a handful of global firms.

https://doi.org/10.1017/dap.2026.10085 Published online by Cambridge University Press

The danger is not that technology companies simply become enemies of states. The danger is more subtle: that they become the infrastructure through which states, firms, and citizens must pass. In that world, sovereignty would remain visible in flags, elections, laws, and budgets, but the architecture of economic possibility would be designed elsewhere. For middle powers, that is the real strategic frontier. Digital sovereignty for middle powers is therefore neither a promise of national technological self-sufficiency nor a simple appeal to multilateral cooperation. It is a strategy for preserving agency under structural asymmetry. Some middle powers will compete for early advantage in compute, data infrastructure, AI investment, and standards. That competition cannot be wished away. But competition without coordination will often leave each of them bargaining separately with larger states and dominant platforms. The more durable strategy is selective coordination: shared standards where scale is needed, domestic capability where exit is essential, and public digital infrastructure where markets alone would convert dependence into permanence. The state as a platform is the institutional form of that strategy, though its instruments will vary from national infrastructure in high-capacity states to pooled procurement, shared standards, and regional public digital infrastructure in more constrained jurisdictions. The task is to remain open without becoming dependent, to exercise control without closing markets, and to build interoperability without surrendering authority. Digital sovereignty, properly understood, is not withdrawal from the world economy. It is the condition for participating in it without being absorbed by it.

Data availability statement. No original datasets were generated, collected, or analysed for this commentary. The manuscript relies on publicly available policy documents, speeches, institutional reports, market reports, and published academic literature cited in the reference list. These materials are available from their respective publishers or issuing organizations; some academic publications or third-party reports may be subject to access restrictions. No replication code is associated with this article.

Acknowledgements. The author acknowledges the use of GPT-5.5 Pro through ChatGPT in May and June 2026 for assistance with language refinement, and reference formatting. The author reviewed, revised, verified, and approved all content and remains solely responsible for the article.

Author contribution. T.W.: conceptualization, formal analysis, methodology, project administration.

Funding statement. Funding statement: This work received no specific grant from any funding agency, commercial or not-for-profit sectors.

Competing interests. Competing interests: The author declares none.

References

Carney M (2026) *Principled and Pragmatic: Canada's Path: Prime Minister Carney Addresses the World Economic Forum Annual Meeting* [Speech transcript]. Prime Minister of Canada. Available at https://www.pm.gc.ca/en/news/speeches/2026/01/20/principled-and-pragmatic-canadas-path-prime-minister-carney-addresses (accessed 20 July 2026).

Cooper AF, **Higgott RA and Nossal KR** (1993) *Relocating Middle Powers: Australia and Canada in a Changing World Order*. Vancouver, British Columbia: University of British Columbia Press.

Couture S and Toupin S (2019) What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society 21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984.

Drezner DW (2007) *All Politics Is Global: Explaining International Regulatory Regimes*. Princeton: Princeton University Press.

European Commission (2023). *Gatekeepers Portal.* Digital Markets Act. Available at https://digital-markets-act.ec.europa.eu/gatekeepers-portal_en (accessed 11 June 2026).

Farrell H and Newman AL (2019) Weaponized interdependence: How global economic networks shape state coercion. *International Security 44*(1), 42–79. https://doi.org/10.1162/isec_a_00351.

Floridi L (2020) The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology 33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6.

Giest S, **McBride K**, **Nikiforova A and Sikder SK** (2025) Digital & data-driven transformations in governance: A landscape review. *Data & Policy 7*, e21. https://doi.org/10.1017/dap.2024.47.

Grieco JM (1988) Anarchy and the limits of cooperation: A realist critique of the newest liberal institutionalism. *International Organization 42*(3), 485–507. https://doi.org/10.1017/S0020818300027715.

Haskel J and Westlake S (2018) *Capitalism without Capital: The Rise of the Intangible Economy*. Princeton, New Jersey: Princeton University Press. https://doi.org/10.1515/9781400888320.

International Energy Agency (2025) *Energy and AI.* Available at https://www.iea.org/reports/energy-and-ai (accessed 20 July 2026).

https://doi.org/10.1017/dap.2026.10085 Published online by Cambridge University Press

Jordaan E (2003) The concept of a middle power in international relations: Distinguishing between emerging and traditional middle powers. *Politikon 30*(1), 165–181. https://doi.org/10.1080/0258934032000147282.

Keohane RO (1984) *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, New Jersey: Princeton University Press.

Khan LM (2017) Amazon's antitrust paradox. *The Yale Law Journal 126*(3), 710–805. Available at https://www.yalelawjournal.org/note/amazons-antitrust-paradox (accessed 20 July 2026).

O'Reilly T (2011) Government as a platform. *Innovations: Technology, Governance, Globalization 6*(1), 13–40. https://doi.org/10.1162/INOV_a_00056.

OECD (2019) *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-Use across Societies*. Paris: OECD Publishing. https://doi.org/10.1787/276aaca8-en.

OECD (2022) *Data Shaping Firms and Markets* (OECD Digital Economy Papers No. 344). OECD Publishing. https://doi.org/10.1787/7b1a2d70-en.

OECD (2024) *Digital Public Infrastructure for Digital Governments* (OECD Public Governance Policy Papers No. 68). OECD Publishing. https://doi.org/10.1787/ff525dc8-en.

Parker GG, **Van Alstyne MW and Choudary SP** (2016) *Platform Revolution: How Networked Markets Are Transforming the Economy and how to Make them Work for you*. New York: W. W. Norton & Company.

Pohle J and Thiel T (2020) Digital sovereignty. *Internet Policy Review 9*(4), 1–19. https://doi.org/10.14763/2020.4.1532.

Rochet J-C and Tirole J (2003) Platform competition in two-sided markets. *Journal of the European Economic Association 1*(4), 990–1029. https://doi.org/10.1162/154247603322493212.

Snidal D (1991) Relative gains and the pattern of international cooperation. *American Political Science Review 85*(3), 701–726. https://doi.org/10.2307/1963847.

Srnicek N (2017) *Platform Capitalism*. Cambridge: Polity Press.

Stevens Y, **Masoodi MJ and Andrey S** (2020) *Home Ice Advantage: Securing Data Sovereignty for Canadians on Social Media*. Cybersecure Policy Exchange. Available at https://cybersecurecatalyst.ca/home-ice-advantage/ (accessed 20 July 2026).

Synergy Research Group (2026) *Cloud Market Annual Revenue Run Rate Topped Half a Trillion Dollars in Q1 as Growth Surge Continues*. Available at https://www.srgresearch.com/articles/cloud-market-annual-revenue-run-rate-topped-half-a-trillion-dollars-in-q1-as-growth-surge-continues (accessed 20 July 2026).

UNCTAD (2021) *Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data Flow*. United Nations. Available at https://unctad.org/publication/digital-economy-report-2021 (accessed 20 July 2026).

Van Dijck J, **Poell T and de Waal M** (2018) *The Platform Society: Public Values in a Connective World*. New York: Oxford University Press.

Waltz KN (1979) *Theory of International Politics*. Massachusetts: Addison-Wesley.

Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

Zwick A and Spicer Z (2024) Examining the smart city generational model: Conceptualizations, implementations, and infrastructure Canada's Smart City challenge. *Urban Affairs Review 60*(4), 1229–1253. https://doi.org/10.1177/10780874231222243.

Cite this article: Warin T (2026). Middle powers in the platform economy: Digital sovereignty after the data pivot. *Data & Policy*, 8: e37. doi:10.1017/dap.2026.10085

https://doi.org/10.1017/dap.2026.10085 Published online by Cambridge University Press