



**AI Data Centres: Community Consultation,
Accountability and Australia's National Interest**

1 September 2026

A submission to the Senate

Environment and Communications References Committee

for its inquiry on Artificial Intelligence and Data Centres

Referred 13 May 2026

Executive Summary and Recommendations

This submission starts with a fundamental question: what rights should affected communities have before major development decisions on AI data centres are made and become difficult to reverse? We also seek to clarify who holds legal responsibility for considering community sentiment and what accountability exists when legitimate concerns are heard but not acted upon? A second departure point is the depth of Australian capability for monitoring international aspects of data centre operations.

AI data centres differ from other large industrial or services infrastructure projects mainly in how intensely and inflexibly they consume energy and water and at unusually high levels; how fast their technology becomes obsolete; and how unevenly their benefits and costs are distributed across the community versus a small set of corporate owners. They also carry elements of economic risk and geopolitical significance that many other infrastructures do not. At a national level, they are regulated under the Security of Critical Infrastructure Act (SOCI Act 2018) but only for the purposes of cyber security, including ownership restrictions, but not for environmental impact.

Australian states and territories are approving large AI data centres without settled answers to basic governance questions. As this submission argues, no detail yet exists on the specific types or methods of consultation likely to be required. Core accountability gaps remain unresolved. These should be closed before, not after, Australia's data-centre footprint expands further.

Two problem sets are addressed in this submission.

First, community and specialist consultation remains procedurally thin and does not conform to reasonable standards articulated in the Senate Committee on the Environment in 1999. Nor do current data centre consultation habits match high standards laid out in international approaches to technology impact assessment or environmental impact assessment that developed in the United States in the 1960s and 1970s and subsequently in Australia. The main failings have been in the depth of the consultations, their lack of comprehensive analysis and their timing.

International evidence shows the cost of regulating after the fact rather than before is considerably higher.

Consistent polling shows majority public opposition to local data centres in key communities in the US and Canada. By August 2026 over 225 local and state moratoriums or restrictions had been recorded across 30 states, including major cities such as Nashville, Louisville, Indianapolis, Seattle and Minneapolis. Social licence cannot be assumed. The policy of the data centre industry in major economies appears to be “accelerate siting, manage friction locally”. In Australia, the Prime Minister waved the patriotism flag, referencing “the Australian way” in his July statement as some sort of reassurance that good will prevail “without ... dividing communities”. This reassurance appears to be of dubious value for residents of George Town in Tasmania in 2026 who opposed two large data centre projects, raising concerns over water and energy consumption and noise pollution, only to be ignored by a local council decision. In Tasmania, such proposals are reviewed by local councils and not state planning agencies as occurs in New South Wales and South Australia for instance. However, there is room to ask whether any level of government in Australia can adequately address local community

concerns, indicating the need for wider and more effective consultation reaching well beyond single communities.

Second, Australia lacks rigorous, ongoing capability to analyse the geopolitics of AI infrastructure. Popular language around "AI sovereignty" obscures rather than clarifies who controls compute, software, data and infrastructure. As policy for Cloud suggests, these are four distinct ownership layers that can be transferred across borders independently of each other. A data centre built on Australian soil, wholly Australian-owned, can still host foreign-controlled compute and remotely governed software. Australia currently has no standing multidisciplinary capability to track these dependencies across the datasphere as they evolve.

The submission recommends two linked reform packages.

Set A: Community and specialist consultation

- A legislated national minimum standard for community consultation
- Mandatory early consultation
- A designated accountable decision-maker
- A genuine causer-pays principle
- Clear, tiered consequences for non-compliance
- Mandatory cumulative precinct assessment
- Population exposure assessment by locality
- Independent baseline and continuous monitoring
- A statutory Community Response Statement.

Set B: Strategic and geopolitical governance capability

- Invest in AI policy expertise well beyond current levels
- Build public equity or co-investment stakes into strategically significant projects
- Diversify supply-chain and jurisdictional dependency rather than trying to eliminate it
- Separate and regulate the four ownership layers explicitly: infrastructure, hardware, software and data.

We need separate regulation of the four ownership layers rather than treating "the data centre" as a single undifferentiated policy object. Australia has discrete instruments touching each layer, but they weren't designed as a coordinated four-layer framework. Capability to monitor two of the four layers (supply-chain dependency and remote administrative control) is thin. The balance between the power of federal government and state governments shifts materially in favour of the federal government if this four-layer approach is followed.

Streamlined approvals and genuine accountability are currently in tension. Given the ongoing monitoring and compliance obligations in play, reversal of a decision to permit data centre construction or continued operation should be an expected outcome, not an exceptional one. Such an outcome will certainly be foreseeable wherever monitored conditions diverge materially from those on which approval was granted. Community expectations for consultation must not be sacrificed to the current "gold rush" mentality for data centre construction and operations or appeals to patriotism.

Contents

Introduction	1
Senate Committee consultation benchmarks	2
Specialist consultation benchmarks	2
Should maximising foreign investment be the driver?	3
Lane Cove provides a current Australian test.....	4
Role of local councils	6
Heat is an emerging impact that warrants assessment	7
Memphis demonstrates why governance should precede operation	7
Community consultation must begin with information	8
Australia’s commitment to the environment as a human-rights issue.....	9
Public acceptance cannot be presumed	10
Frontier AI developer argues for preserving options to slow development.....	11
Streamlining with democratic governance	11
Australian capability for rigorous geopolitical analysis of AI data centres	12
Recommendations	17
Set A: An enforceable social licence for hosting communities.....	17
Set B: Strategic and geopolitical governance capability	18

Introduction

The Federal Government has sought to create nation-wide standards for AI data centre construction and operation through its March 2026 *Expectations*¹ document and its July 2026 commitment to an "enforceable social licence".² Its preferred tool has been a set of "Standards" rather than legislation. At the time of writing, the National Cabinet had just met (26 August 2026)³ and acknowledged the commitment of the federal government to develop consistent mandatory standards in principle and that these efforts would be "designed to complement, not duplicate, state and territory planning and approval processes".

At present, Commonwealth policy for data centres principally describes what developers should do but with little formal legal scaffolding against the backdrop of growing community concerns and contestation. Existing state planning laws provide formal opportunities for communities to make submissions. What is less clearly defined is what communities must be told before decisions are made; how early they must be consulted; who independently evaluates the concerns they raise; how cumulative impacts are assessed; what must change when evidence identifies a material risk; and what consequences follow where consultation occurs procedurally but does not meaningfully influence the final decision.

This submission does not propose that communities should have an automatic veto over nationally significant infrastructure. Rather, where local stakeholders will bear the consequences of national technology policy, the Australian political system should provide for high standards of consultation with them, especially to ensure that specialist opinion from all of Australia and input from our international partners are included in the process. Such consultations should serve at least three purposes: to identify the decision makers accountable for the long-term implementation of the proposed projects; to comprehensively assess their social and political costs and risks, and to establish enforceable regimes of compliance proportionate to those risks.

This submission is made to the Parliamentary Inquiry into Artificial Intelligence and Data Centres, being conducted by the Senate Environment and Communications References Committee.⁴ The submission is a collective effort of several Fellows and advisers of the Social Cyber Institute. It does not reflect a formal position of the Institute.⁵

¹ Australia. Department of Industry, Science and Resources. "Expectations of Data Centres and AI Infrastructure Developers". 23 March 2026. <https://www.industry.gov.au/NationalDataCentreExpectations>.

² Anthony Albanese (Prime Minister of Australia). "AI: Australia's Interests" (media statement). 15 July 2026. <https://www.pm.gov.au/media/ai-australias-interests>.

³ Australia. Prime Minister. "Statement following the meeting of National Cabinet". 26 August 2026. <https://www.pm.gov.au/media/meeting-national-cabinet-26-august-26>.

⁴ Australia. Senate. Environment and Communications References Committee. "Artificial intelligence and data centres". Referred 13 May 2026. https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/Aldatacentres48P. The terms of reference are:

"Artificial intelligence and data centres, with particular reference to:

1. the effectiveness of existing regulatory frameworks in managing the growth of data centres in Australia, including in relation to existing and future deals between the Government and global Artificial Intelligence (AI) companies;
2. the potential impacts of AI and data centres on Australian communities, industries and the environment, water and energy; and
3. any other related matters."

⁵ Authors include Professor Greg Austin, Adjunct Professor, University of Technology Sydney and Director of Research, Social Cyber Institute; Clare Boyd, Adviser to the Board, Social Cyber Institute; and Dr Gary Waters, Distinguished Fellow, Social Cyber Institute. Reviewers include Professor Glenn Withers, Chair, Social Cyber Institute

Senate Committee consultation benchmarks

In 1999, the Senate Environment, Communications, Information Technology and the Arts References Committee published its report on Commonwealth Environment Powers.⁶ The report discussed or proposed standards for community consultation on environmental policy, as set out in Table 1. Importantly, the Committee was not controlled by the Coalition Government. Although the Coalition held a majority in the House of Representatives, it did not hold a majority in the Senate. The Committee was chaired by Australian Democrats Senator Lyn Allison and comprised three Labor senators and two Liberal senators.

Table 1: Proposals in 1999 for Standards Community Consultations

Requirement
1. Involve the community at the scoping stage, before the assessment is prepared
2. Publicly advertise a notice of intention describing the proposal and inviting submissions on its likely environmental significance
3. Allow the public to comment on whether the proposal is likely to have a significant effect on the environment
4. Allow any person to refer the proposal to the relevant authority for a significance determination
5. Keep participation ongoing, rather than limiting it to comments on a completed assessment document
6. Provide transparent participation arrangements so the community can contribute to environmental decision-making and trust the assessment system
7. Preserve access to legal review by avoiding barriers to public challenges to governmental decisions and breaches of environmental law
8. Ensure community and conservation groups have adequate resources to make timely submissions

Across Recommendations 21-29, the Committee advocated a broader Commonwealth role in environmental assessment, public participation and national standards. It did not prescribe detailed consultation procedures, but emphasised early public involvement, open referral rights, transparency, review mechanisms and adequate resourcing. Several recommendations strengthening Commonwealth oversight and public participation, including Recommendations 21, 24 and 26, were not adopted by the Federal government in the form proposed. Recommendation 28 supported accreditation of State and Territory processes where they provided equivalent environmental protection.

Specialist consultation benchmarks

Affected communities are not the only stakeholders relevant to the decision about the value and risks of building data centres. International practice recognises an important role for scientific experts and civil society organisations in environmental consultations of regional or national significance. Their expertise can inform issues such as national security, resources and climate impacts, economic viability, social impacts and future trends. This broader

and Emeritus Professor at the Australian National University; Laura Zimmerman, CEO and Founder McIntye Health; and Professor Dan Svantesson, Faculty of Law (Bond University) and a co-director for the Centre for Space, Cyberspace and Data Law (CSCDL).

⁶ Australia. Senate Environment, Communications, Information Technology and the Arts References Committee. "Commonwealth Environment Powers Inquiry". 1999.

https://parlinfo.aph.gov.au/parlInfo/download/publications/tailedpapers/8725/upload_pdf/HPP042016001176.pdf.

approach to environmental impact assessments has been established in jurisdictions for decades. It is also reflected in the Australian Government-funded research on technology impact assessment (TIA) for peace and stability and led in Australia by the Social Cyber Institute.⁷ That work promoted the following benchmarks for effective TIA:

- the scope and granularity of the technology being assessed
- the depth and detail of specialist input
- recognition of the significant role of non-technical social, political, legal and economic impacts
- the breadth and depth of stakeholder input
- the comprehensiveness of the analysis, which should include international and alternative perspectives
- the timeliness of the assessment
- a need for clarity about the ethical frameworks to be applied.⁸

This two year study identified three key weaknesses in Australian approaches:

- the technology assessment work was largely left to parliamentary committees
- even this mechanism was rarely used
- parliamentary examination tended to be relatively superficial, focussing more on AI as an aggregated set of technologies rather than on the distinct implications of the many sub-fields of AI.

Should maximising foreign investment be the driver?

Australia's National AI Plan⁹ seeks to increase productivity, investment and national capability. These are legitimate objectives. However, there is substantial uncertainty regarding the timing and scale of AI-driven productivity gains. The Reserve Bank of Australia's engagement with Australian firms has identified expectations of longer-term productivity improvement alongside uncertainty about return on investment, implementation and when material benefits will emerge.

The Social Cyber Institute's earlier research similarly identified increasing electricity, water and resource demands associated with AI infrastructure and uncertainty regarding its longer-term social and economic consequences.¹⁰

⁷ Social Cyber Institute, 'Technology Impact Assessment for Peace and Stability: A Comparative Study on Australia and India', June 2025, p. ii,

https://www.socialcyber.co/files/ugd/15144d_c5acc66a4a014035a939a1b534f06822.pdf.

⁸ G. Austin *et al.*, "Key Dimensions in Technology Impact Assessment for Peace and Stability: Australia and India," in *IEEE Transactions on Technology and Society*, 2026, doi: 10.1109/TTS.2026.3718558.

⁹ Australian Government, Department of Industry, Science and Resources, National AI Plan, 2 December 2025, <https://www.industry.gov.au/publications/national-ai-plan>.

¹⁰ AI data centres can be very large local water users but they are not automatically more water-intensive than manufacturing plants overall. The comparison depends on the facility's size, cooling technology, production process, climate and whether indirect water used for electricity generation is included. Data centres can create a distinctive local impact because they:

- operate continuously, 24 hours a day
- require a relatively constant supply
- may consume a high proportion of withdrawn water through evaporation
- can create sharp peak demands
- are often located near urban communities where water systems are already heavily used
- may be clustered in the same precinct.

This points to the need for a broader assessment of economic costs and benefits, including:

- additional grid infrastructure
- water infrastructure
- health expenditure associated with environmental exposure
- environmental remediation
- lost productivity associated with poor health or environmental stress
- opportunity costs where electricity, land, water or network capacity cannot be deployed elsewhere

These remain economic costs even when they are externalised from a developer's budget plan or balance sheet.

Clean air, secure water, reliable and affordable energy, a stable climate and a healthy population are productive national assets. They are not competing objectives to economic prosperity; they are among its foundations.

Australia should seek to remain an attractive destination for high-quality AI investment. However, regulatory certainty should not be confused with regulatory concession.

Faster and clearer approval pathways may improve investment confidence, but the relevant national-interest question is not simply how much capital Australia can attract. It is what conditions will ensure that investment produces enduring Australian value while its infrastructure costs are appropriately allocated between service providers and the public.

The Government's own expectations identify Australian skills, jobs, research capability, supply chains and local participation as important outcomes. At the same time, major data-centre investment should be assessed not only by headline capital expenditure, but by its contribution to Australian capability and its net public benefit across economic, infrastructure, environmental, security and community dimensions, including energy and water demand.

A predictable national framework can support investment certainty while affirming governance and public confidence.

Lane Cove provides a current Australian test

The emerging concentration of data centres at Lane Cove West provides a practical Australian example of why this issue requires immediate attention.

Goodman Group's proposed Project Mars at 12 Mars Road would operate 24 hours a day, seven days a week, with power consumption of up to approximately 90 MW.¹¹ It will consume 1,405 kilolitres of potable water and produce 468 kilolitres of wastewater every day. The "application, environmental impact statement, and accompanying documents" were posted for exhibition from Friday 27 March 2026 until Tuesday 5 May 2026. At the time of publishing this notice, the Minister for Planning and Public Spaces had "not directed that a public hearing should be held" in spite of significant potential questions about the viability of the project. By 1 September 2026, only eight of 374 submissions supported the project. (It should be noted that "unique

¹¹ Goodman Group. "Project Mars, 12 Mars Road" (project documentation), 2026, <https://au.goodman.com/property-lease-site/project-mars>.

objections” rather than a raw count of individual objections is considered to carry procedural weight.)

Project documentation is extensive,¹² comprising hundreds of documents and technical reports that may be difficult for non-specialist members of the public to navigate. Nevertheless, important gaps appear to remain in the comprehensiveness of the information available, notably the apparent absence of an accessible, integrated analysis of the project’s local electricity and water demands and their cumulative environmental impacts. Of note, the initial EIS appears to misrepresent a stormwater plan (Appendix X) as an “Integrated Water Management Plan”.¹³

By 30 April, Sydney Water¹⁴ wrote:

“Sydney Water is unable to support progression of SSD-82052708 without further study outputs. The proponent has entered into a Sydney Water Planning Agreement to undertake a detailed Planning assessment to assess water demand options and wastewater impact. It is anticipated that the planning assessment will commence imminently and conclude in Q4 2026. Accordingly, it is requested that DPHI defer SSD-82052708 and re-refer once outcomes of the assessment have been finalised.

In other words, the constraint is that the existing drinking-water network in the Chatswood supply zone (servicing Lane Cove) may not be able to actually carry this extra daily load of the new data centre, a situation compounded by the fact several other data centres in the same precinct are or may be drawing on the same water supply zone.

Lane Cove Council states that one data centre is operating in Lane Cove West and three additional facilities are proposed.¹⁵ Official NSW Government records also identify a fifth, preliminary proposal by Lane Cove DC Alliance at 16–20 Mars Road, which has been endorsed to progress through the Investment Delivery Authority. This endorsement is not planning approval.

Critically, the Council has stated that no cumulative assessment has been provided of what the group of four or five data centres together will demand from local water, electricity and road networks.¹⁶

That raises a national policy question:

If major developments are assessed individually, even those within one large city precinct, who is responsible for determining when their combined effect becomes material or unacceptable?

¹² See NSW Major Projects Planning Portal, <https://www.planningportal.nsw.gov.au/major-projects/projects/project-mars-data-centre>. Hundred of documents can be found there.

¹³ See “Project Mars Data Centre 12 Mars Road, Lane Cove West Stormwater Report”, December 2025, <https://majorprojects.planningportal.nsw.gov.au/prweb/PRRestService/mp/01/getContent?AttachRef=SSD-82052708%2120260218T235844.849+GMT>. This appears to have been labelled in the covering document as an “integrated water management plan”, which it clearly is not.

¹⁴ See Letter from Sydney Water to the Department of Planning, Housing and Infrastructure, 26 April 2026, <https://majorprojects.planningportal.nsw.gov.au/prweb/PRRestService/mp/01/getContent?AttachRef=EXH-110951999%2120260506T061135.839+GMT>.

¹⁵ Lane Cove Council, “Have Your Say: Data Centre Proposed for 12 Mars Road”, 21 April 2026, <https://www.lanecove.nsw.gov.au/Council-News/Have-Your-Say-Data-Centre-Proposed-for-12-Mars-Road>.

¹⁶ Lane Cove Council. “Major Projects Council Submission Project Mars Data Centre (SSD-82052708) (Lane Cove)”. 20 April 2026. <https://ecouncil.lanecove.nsw.gov.au/trim/DocumentLink.asp?ReclId=28938/26>, p. 1.

Residents do not experience planning on a project-by-project basis. They experience the physical environment produced collectively by all developments operating around them.

For communities, the relevant exposure is cumulative: combined operational noise; combined electricity and water demand; combined backup-generation capacity and emissions; combined construction activity; combined heat rejection;¹⁷ and combined effects on local infrastructure, vegetation and amenity. National standards should therefore require forward-looking cumulative assessment wherever multiple facilities exist, are approved, or are reasonably foreseeable within the same precinct. Planning standards from the NSW government already require comprehensive precinct-level EIS, not just specific to a single project

Assessment should also identify the population potentially exposed to those effects.

This should not mean declaring everybody within an arbitrary distance to be “affected” or “harmed”. It should mean using Australian Bureau of Statistics population data together with site-specific acoustic, air-dispersion and thermal modelling to determine how many residents, schools, health facilities and other sensitive receptors are located in areas where modelling predicts measurable effects, at what level and for what duration. That information should be available to both decision-makers and communities before approval.

Role of local councils

Lane Cove also raises a broader question about the formal role of local government. Local councils hold detailed knowledge of local road networks, housing and development pressures, schools and community facilities, waterways, biodiversity, existing industrial activity and the practical capacity of local infrastructure.

Lane Cove Council’s identification of cumulative issues across several proposed facilities illustrates the value of that local institutional knowledge.

If the Commonwealth intends to establish nationally consistent standards governing where major data centres are appropriately located, the national framework should clarify how local-government evidence is incorporated into the decision-making process, which authority is responsible for responding to it and how differences are resolved between Commonwealth, State or Territory and local assessments (community or Council).

This need not give councils a unilateral veto. It should give their evidence a defined place within the governance framework. But opponents have few other places to go as the decision by six of seven Councillors of George Town in Tasmania to override significant local opposition toward two large data centre projects on 25 August shows.¹⁸ The dissenters were given fourteen days by the Council to appeal the decision through a particularly narrow almost useless mechanism. So, to be effective, local sentiment opposed to data centre siting or operations needs to be buttressed by wider and more effective consultation across the community that extends well

¹⁷ “Heat rejection refers to the process of transferring heat from a cooling system, such as an absorption chiller, to the ambient environment, typically using methods like wet cooling towers that utilize water or dry cooling systems that circulate air.” See Science Direct, “Heat Rejection”, <https://www.sciencedirect.com/topics/engineering/heat-rejection>.

¹⁸ Ashleigh Barraclough. "Firmus 288-Megawatt AI Data Centre at Bell Bay, Tasmania Gets Approval After 6-1 Council Vote." *ABC News*. 26 August 2026. <https://www.abc.net.au/news/2026-08-25/firmus-ai-bell-bay-receives-george-town-council-approval/107074336>.

beyond the local council jurisdiction, perhaps aiming at national and even international mobilisation.

Heat is an emerging impact that warrants assessment

Waste heat is one example of an impact that has received comparatively limited attention in Australian data-centre planning. There is now evidence that off-site thermal effects can be measurable.

A 2026 peer-reviewed study of operational data centres in metropolitan Phoenix reported average downwind air temperatures approximately 0.7–0.9°C higher than corresponding upwind areas, with maximum measured warming of 2.2°C and detectable thermal signatures up to approximately 500 metres from facility boundaries.¹⁹

Separate international research released in 2026 using satellite land-surface-temperature data reported an average post-operation increase of approximately 2°C around AI data centres, with site-level estimates ranging from approximately 0.3°C to 9.1°C and a measurable land-surface-temperature signal reported at distances of up to 10 kilometres, with the effect diminishing with distance.²⁰ The latter research is currently a preprint and has not yet completed peer review. Its upper estimates should therefore not be presented as predictions for Lane Cove or any Australian facility.

Its policy significance is nonetheless important. A potentially material environmental effect has been identified. The appropriate response is not to assume that it will occur at Lane Cove at the reported magnitude. It is to require developers to establish pre-development temperature baselines, undertake site-specific thermal modelling and monitor actual conditions after operations commence.

Heat is also relevant beyond environmental amenity. The World Meteorological Organisation recognises high temperatures as a public-health risk that can aggravate cardiovascular, respiratory, kidney and mental-health conditions.²¹ It is one reason why environmental effects should not be assessed separately from economic consequences.

Memphis demonstrates why governance should precede operation

xAI's development in the Memphis metropolitan area, including its Colossus 2 project near the Tennessee-Mississippi border, provides an important international case study. A July 2026 Reuters investigation reported that xAI had installed 59 natural-gas turbines associated with its Colossus 2 infrastructure without federal air permits.²² Based on manufacturer information for 30 of the turbines, Reuters calculated that those 30 turbines could emit approximately 2,500 short tons of nitrogen oxides, 4,000 short tons of carbon monoxide and 22 short tons of formaldehyde annually, assuming continuous operations at 80 per cent.

¹⁹ Sailor D., Abolhassani S.S. and Martin E. P. "Data Center Waste Heat as an Emerging Urban [Environmental Effect]." *Journal of Engineering for Sustainable Buildings and Cities (ASME)*, vol. 7, no. 2, art. 024501, 2026, <https://asmedigitalcollection.asme.org/sustainablebuildings/article/7/2/024501/1233035/Data-Center-Waste-Heat-as-an-Emerging-Urban>.

²⁰ DigNetSol. "Sustainability Tech: AI Data Centres May Heat Surrounding Areas for Miles". 2026 (preprint, not yet peer-reviewed). <https://dignetsol.co.uk/news-resources/sustainability-tech-ai-datacentres-may-heat-surrounding-areas-miles>.

²¹ World Meteorological Organization. "Extreme Heat." Geneva: WMO. <https://wmo.int/themes/extreme-heat>.

²² Reuters. "Anthropic Says AI Labs Need Coordinated Plan to Halt Development if Risks Rise". 4 June 2026. <https://www.reuters.com/business/anthropic-says-ai-labs-need-coordinated-plan-halt-development-if-risks-rise-2026-06-04/>.

The legal position concerning permitting has been contested by xAI, regulators and environmental and civil-rights organisations.

Reuters examined government health data for census tracts within five miles of the turbine location and reported asthma prevalence above the corresponding county rates in 27 of 28 tracts²³ and COPD prevalence above county rates in 24. Those health conditions largely predated xAI and cannot properly be attributed to the facility. Their significance is different: large new combustion infrastructure was introduced into communities already carrying comparatively high respiratory-health burdens.

Other evidence has been mixed. Initial testing commissioned by the City of Memphis did not identify dangerous pollutant concentrations at the sampled locations during the periods tested, while other analyses have reported changes in nitrogen-dioxide concentrations near the broader development area. Attribution is complicated by other industrial pollution sources. That uncertainty is itself instructive. Communities should not have to resolve disputes about their baseline health conditions, air quality, emissions or exposure through competing studies and litigation after major infrastructure is already operating.

For Australia, the governance lessons are straightforward:

- relevant baseline environmental conditions should be established before development
- foreseeable emissions should be independently modelled
- monitoring should continue during operation
- the information should be publicly accessible
- communities should know which authority is responsible for acting if actual conditions differ materially from those approved.

Community consultation begins with comprehensive information

Meaningful consultation requires communities to have access to a comprehensive suite of information necessary to understand the potential consequences of a development.

For major AI data centres, consultation should therefore include clear information about:

- maximum and expected electricity demand;
- water consumption and cooling systems;
- backup-generation capacity, fuel source and anticipated operation;
- modelled air emissions;
- operational and cumulative noise;
- waste heat and potential off-site thermal effects;
- additional electricity, water and transport infrastructure required;
- existing environmental and relevant population-health conditions; and
- cumulative impacts of other existing, approved and reasonably foreseeable data centres.

²³ The word "tracts" is short for census tracts, a standard unit the US Census Bureau uses to divide counties into smaller, relatively stable geographic areas for statistical purposes. Each tract typically contains somewhere in the range of 1,200–8,000 people, designed to be small enough to reflect a homogeneous local population but large enough to support reliable statistics. See United States. Census Bureau. Geography Program Glossary. "Census tracts". https://www.census.gov/programs-surveys/geography/about/glossary.html#par_textimage_13.

New South Wales already requires State Significant Development applications to undergo public exhibition, generally for at least 28 days. Submissions are received and published, proponents respond to issues raised and decision-makers are required to consider community views. These processes should allow for meaningful safeguards provided the information provided is comprehensive rather than neatly tailored to appear like consultation.

Most importantly, an enforceable social licence requires Parliaments to consider what happens once submission is made.

A national framework should require a transparent Community Response Statement identifying:

1. the material concerns raised;
2. the evidence used to investigate them;
3. any changes made to the project;
4. concerns that were not accepted and the evidence supporting those decisions;
5. conditions imposed to manage identified risks; and
6. the regulator or decision-maker responsible if actual impacts subsequently exceed those approved.

This would not make community opinion determinative. It would make the responsible authority accountable for demonstrating that consultation has materially informed the decision-making process rather than merely accompanying it.

Australia's commitment to the environment as a human-rights issue

On 28 July 2022, the United Nations General Assembly recognised the human right to a clean, healthy and sustainable environment, adopting Resolution 76/300 by 161 votes in favour, none against and eight abstentions.²⁴ Australia voted in favour of the resolution.

The resolution does not itself create a directly enforceable domestic right in Australia and does not provide communities with a legal veto over infrastructure development. Its policy relevance is nevertheless significant.

Australia has expressly supported international recognition that a clean, healthy and sustainable environment is integral to human wellbeing. Clean air, safe water, a sustainable environment and protection from harmful pollution are closely connected with the enjoyment of rights to life and health.

This commitment is also relevant to Australia's regional policy settings. Australia has recognised climate change as the 'single greatest threat' to the livelihoods, security and well-being of Pacific peoples.²⁵ As Australia expands energy-intensive AI infrastructure domestically, maintaining consistency between its domestic environmental settings and the climate and security principles it promotes across the Pacific is relevant to both policy coherence and regional credibility.

²⁴ Environmental Defenders Office (EDO). Summary of UN General Assembly Resolution 76/300: The Human Right to a Clean, Healthy and Sustainable Environment, August 2022, https://www.edo.org.au/wp-content/uploads/2022/08/EDO_HealthyEnvironment_Summary_Web.pdf.

²⁵ Australia. Department of Foreign Affairs and Trade. "Climate Change and Resilience." Canberra: Australian Government. <https://www.dfat.gov.au/geo/pacific/development-assistance/climate-change-and-resilience>.

Where an infrastructure proposal may materially affect air quality, environmental noise, local temperatures, water systems or surrounding ecosystems, community participation is therefore more than a matter of planning courtesy. It is relevant to ensuring that the environment and health considerations are properly understood before decisions are made.

Affected communities should have timely access to relevant information and a meaningful opportunity to participate in decisions concerning the environment in which they live.

For major data-centre developments, this strengthens the case for consultation requirements that are early, informed and capable of influencing decision-making, particularly where potential environmental impacts extend beyond the development site.

Public acceptance cannot be presumed

The importance of meaningful consultation is reinforced by evidence from other democracies. A Gallup survey conducted in March 2026 found that 71 per cent of Americans opposed construction of an AI data centre in their local area, including 48 per cent who strongly opposed it.²⁶ Opposition extended across political affiliations.

An Angus Reid survey in June 2026 similarly found that 68 per cent would oppose a large AI data centre within a few blocks of their home and 68 per cent said government should heavily regulate AI even if doing so slowed development while substantial majorities supported strong government regulation.²⁷

These results should not be described as proof of general population opposition to data centres. They demonstrate something more directly relevant to government: local social consent cannot be assumed based on investment announcements, technological demand or national economic strategy.

Other democracies have already adjusted policy after rapid data-centre expansion created material resource constraints.

In Ireland, data-centre electricity consumption increased from approximately 5 per cent of metered electricity in 2015 to approximately 23 per cent by 2025. Ireland has subsequently strengthened electricity connection requirements for new data centres, including requirements relating to generation and/or storage capacity.

The Netherlands has strictly regulated the location of new hyperscale data centres, limiting development to specified areas in response to constraints on land and energy.

In Chile, environmental concerns about water use during prolonged drought led to further environmental assessment of Google's proposed Santiago data centre and the subsequent redesign of its cooling system from water-based to air-cooled technology.

These jurisdictions are not rejecting digital infrastructure. Their experience demonstrates the value of addressing resource constraints and environmental impacts before rapid developments make them more difficult to manage. Australia has an opportunity to learn from jurisdictions that have already experienced rapid data-centre expansion. The evidence should

²⁶ Jones J. "Americans Oppose AI Data Centers in Their Area." *Gallup News*, 13 May 2026.

<https://news.gallup.com/poll/709772/americans-oppose-data-centers-area.aspx>.

²⁷ CBC News. "AI Data Centre Opposition. Explained" (reporting Angus Reid Institute survey, June 2026).

<https://www.cbc.ca/news/canada/ai-data-centre-opposition-explained-9.7225796>.

inform policy before Australia reaches the same level of infrastructure concentration. If its objective is to strengthen the economy it would be counterproductive to pursue rapid expansion first and then incur public and private costs to addressing avoidable pressure on energy, water, health infrastructure and the environment. A stronger economic approach is to incorporate those lessons into the regulatory framework now, so that growth is both investable and sustainable.

Frontier AI developer argues for preserving options to slow development

There is a final consideration relevant to the pace of infrastructure development.

Anthropic, one of the world's leading frontier AI developers and a company with which the Australian Government announced formal collaboration in 2026,²⁸ has argued that the world should preserve the capacity to slow or temporarily pause frontier AI development under credible international coordination if technological development begins to outpace governance and societal safeguards.²⁹ Anthropic has not called for an immediate unilateral global freeze. That distinction is important. Its position is nevertheless significant because it demonstrates that concern about the speed of AI development is not confined to external critics of the technology. It exists within the frontier industry itself. This has implications for infrastructure policy.

Data centres are not simply passive infrastructure responding to AI growth. Compute capacity is one of the physical inputs that determines the scale and speed at which increasingly advanced AI systems can be developed and deployed.

Long-term commitments involving land, electricity generation, transmission, water and major data-centre precincts should therefore preserve regulatory flexibility rather than assume continued growth in future compute demand is inevitable or automatically in the national interest, or indeed, more broadly in the long-term interest of humanity.

Streamlining under democratic governance

The Government has also identified faster approvals and streamlined compliance as objectives of a nationally consistent framework. That objective need not conflict with good governance. Streamlining should mean removing unnecessary duplication, not reducing scrutiny. A national framework can improve investment certainty by establishing common evidence requirements, clear responsibilities and predictable assessment pathways. However, community consultation, environmental and cumulative-impact assessment, access to evidence and transparent reasons for decision-making should remain substantive safeguards.

Parliament should therefore clarify which processes are intended to be streamlined and which protections will remain non-negotiable.

If assessment pathways are accelerated, the framework should also ensure that local residents have sufficient information, time and opportunity to participate meaningfully before decisions are made. This is particularly important because the Government is simultaneously seeking faster and more predictable approvals and an enforceable social licence. Those objectives can

²⁸ Australian Government and Anthropic. Memorandum of Understanding between the Australian Government and Anthropic on Collaboration on AI Opportunities. 1 April 2026. <https://industry.gov.au/publications/memorandum-understanding-between-australian-government-and-anthropic-collaboration-ai-opportunities>.

²⁹ Reuters. "Anthropic Says AI Labs Need Coordinated Plan to Halt Development if Risks Rise." 4 June 2026. <https://www.reuters.com/business/anthropic-says-ai-labs-need-coordinated-plan-halt-development-if-risks-rise-2026-06-04/>.

coexist, but only if community participation is designed into the streamlined framework rather than being diminished by efforts to accelerate it.

A streamlined system should therefore be judged not only by the speed of approvals, but by whether it preserves transparency, accountability and meaningful participation within Australia's existing democratic and regulatory framework.

Australian capability for rigorous geopolitical analysis of AI data centres

We know that AI has potentially significant implications for global economic and strategic interests. Yet Australia does not currently appear to have an organised framework for analysing these issues, nor a settled understanding of the key questions involved. Moreover, the growing use of the term "AI sovereignty" can obscure rather than clarify the underlying questions of ownership, control, dependency and strategic power. The risk is that describing a capability as "sovereign" may discourage sufficiently rigorous examination of whether it in fact increases Australian autonomy or merely changes the form of external dependency.

The term "sovereignty" is above all a legal doctrine, developed principally in relation to the rights, duties and authority of states under international law. While the condition of sovereignty for a state has certain aspects that can be measured, such as defined borders or effective administrative control of a population, interpretation of these qualities has also historically been shaped by political and legal circumstances. It has been applied as a combination of principle and the practice of states. Sovereignty as concept was always a totality. It has been the sum of its parts but never complete without all of its parts.

Newer concepts such as 'data sovereignty', 'digital sovereignty' and 'AI sovereignty' have little or no connection to the international law concept of sovereignty,³⁰ and are therefore of limited analytical value when assessing the actual distribution of AI power. A more useful approach is to examine the underlying relationships through the concepts of geopolitics and geoeconomics.

The British East India Company is sometimes invoked as an example of a private actor derogating from a state's sovereignty, but this is more precisely explained by the fact that the Company was progressively vested with delegated sovereign functions, such as a royal charter, treaty-making power with local rulers and eventually tax collection. Even though the Company eventually disposed of private coercive capacity,³¹ its paramilitary forces were downstream of that delegated public authority, not the source of it.

This is not to say that concepts related to digital sovereignty are without value but rather that their value lies in geopolitics and geoeconomics, not international law. Structural power theory offers a more precise account of when private infrastructure dependency becomes a genuine strategic vulnerability: control over production, finance, security and knowledge infrastructures can shape state outcomes without requiring formal coercive or legal authority.³² Farrell and Newman's account of "weaponized interdependence" sharpens this further, showing how *states*, not the corporations

³⁰ Svantesson, Dan, 'A Starting Point for Re-thinking "Sovereignty" for the Online Environment', in Anupam Chander, and Haochen Sun (eds), *Data Sovereignty: From the Digital Silk Road to the Return of the State* (New York, 2023; online edn, Oxford Academic, 14 Dec. 2023), <https://doi.org/10.1093/oso/9780197582794.003.0003>, accessed 24 Aug. 2026.

³¹ Stern, Philip J. *The Company-State: Corporate Sovereignty and the Early Modern Foundations of the British Empire in India*. Oxford: Oxford University Press, 2011.

³² Strange, Susan. *States and Markets*. 2nd ed. London: Pinter Publishers, 1994.

themselves, can exploit network centrality in privately-owned infrastructure (financial messaging systems, cloud platforms, chip supply chains) to coerce other states.³³

On this view, persistent corporate non-compliance with a host government's regulations is not a derogation of that state's sovereignty; it is a regulatory and enforcement problem, addressed through ordinary legal powers rather than sovereignty doctrine. A corollary is that a state does not "strengthen" its sovereignty, in the legal sense, merely by reducing dependence on a given foreign corporation even though it may well strengthen its resilience and strategic autonomy. These are legitimate policy goals even if the vocabulary linking them to sovereignty is imprecise. The more useful question is empirical rather than definitional: is there a foreign state positioned and willing to exploit a given dependency and thereby exercise a derogation of sovereignty of that second state? Defence of sovereignty on this front should therefore focus on foreign state conduct and intent not on corporate observance of public law and without treating a commercial technology dependency as inherently a threat to sovereignty.

Notably, this loose usage is not confined to critics or commentators. It is the organising language of government policy itself. Australia's National AI Plan frames "building sovereign capability in AI" as central to national resilience and competitiveness.³⁴ The Government's memorandum of understanding with Anthropic explicitly required the company to align its Australian operations with the Government's own expectations of data centres and AI infrastructure developers.³⁵ This confirms the descriptive point above. This is industrial policy borrowing sovereignty's vocabulary, not sovereignty in the international law sense.

Governments frequently deploy "digital" or "AI sovereignty" as a political signal of resolve rather than a description of any real change in dependency. France illustrates this well: its flagship "cloud de confiance" ("trusted cloud") scheme, launched to guarantee sovereign, French-controlled cloud infrastructure, in practice licenses the underlying technology from Microsoft and Google themselves, through joint ventures such as Bleu and S3NS.³⁶ Nevertheless, France seeks to apply the "sovereign" label over infrastructure still built on and dependent on, the same two American hyperscalers.³⁷ This pattern where sovereignty rhetoric is attached to schemes that leave the underlying dependency largely intact suggests such claims often function as a nationalist political gambit rather than a substantive shift in the distribution of technological control.

We would like to introduce two concepts related to AI sovereignty that shed some light on the geopolitics and geoeconomics of AI data centres. In doing so, the submission questions whether conventional discussions of AI sovereignty adequately capture the dependencies created by ownership of compute infrastructure, cloud services and advanced AI accelerators. The more difficult questions concern who controls these assets, where decision-making power resides and the extent to which states remain dependent on a small number of globally dominant technology companies.

³³ Farrell, Henry, and Abraham L. Newman. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." *International Security* 44, no. 1 (2019): 42–79.

³⁴ Australian Government, Department of Industry, Science and Resources, "Ministers' Foreword," National AI Plan, 2 December 2025, <https://www.industry.gov.au/publications/national-ai-plan/ministers-foreword>.

³⁵ Australian Government and Anthropic, Memorandum of Understanding between the Australian Government and Anthropic on Collaboration on AI Opportunities, 1 April 2026, <https://industry.gov.au/publications/memorandum-understanding-between-australian-government-and-anthropic-collaboration-ai-opportunities>.

³⁶ See N. Bouchard. "The AI Sovereignty Paradox: France and the Limits of Digital Autonomy". Social Cyber Institute. August 2026. p. i. In publication.

Euronews. "France Wants Microsoft, Google to License Cloud Technology to French Rivals." 17 May 2021. <https://www.euronews.com/next/2021/05/17/us-france-cloud>.

³⁷ Businesswire. "Thales and Google Cloud Announce Strategic Partnership to Jointly Develop a Trusted Cloud Offering in France." 5 October 2021. <https://www.businesswire.com/news/home/20211005005894/en/Thales-and-Google-Cloud-Announce-Strategic-Partnership-to-Jointly-Develop-a-Trusted-Cloud-Offering-in-France>.

The first reference point is an analysis of “compute sovereignty” which suggests that the best that “many mid-size and non-aligned states” can hope for “does not involve full-self-sufficiency or domestic control but navigating dependencies in a way that simultaneously preserves autonomy and reduces vulnerability”.³⁸ The article’s core premise is that the questions of “where AI compute is located, who owns it and who governs it” are “central geopolitical questions”. This analysis suggests that compute power can be usefully measured with reference to a census of a country’s “cloud regions” which have access to AI accelerators sufficiently powerful “for both training and inferencing”. A compute region is defined as “an organisational designation for a cluster of interconnected data centres called ‘availability zones’, within a specific bounded territory “named after a nearby city.”³⁹

The study finds that a central geopolitical question is the extent to which states depend on one or more of three major centres of technological power: the US, China or the European Union. The authors conclude that Australia can exercise a “type of sovereignty” through reliance on a single foreign provider that constitutes “selective interdependence with an ally perceived to be politically stable, technologically advanced and ideologically aligned”.⁴⁰

The study then raises a further question directly relevant to Australian data-centre policy: where is cloud compute power located, who owns it and who governs it? In answering the first of these questions, it might be tempting to assume that since the data centres are located in Australia, the “compute power” is necessarily Australian. However, the authors address alternative interpretations of how this question might be answered that challenge any such assumption.

Box 1 (next page) draws on Microsoft sources to illustrate how data hosted in Australian data may nevertheless be transferred or accessed internationally. The most precise and defensible formulation is neither “located in Australia” nor “globally networked” alone. The physical compute substrate is located in Australia, while the system it belongs to may remain part of a globally operated architecture whose broader functions and dependencies vary by service and configuration. “Located in Australia” is true of the hardware in the narrowest physical sense; it does not, by itself, establish Australian ownership, operational control or complete technological independence. Microsoft does offer Australian data residency options for relevant services, but the applicable guarantees must be assessed service by service.

Beyond the location and movement of data, there are questions of ownership of the data, the software, the physical infrastructure and the data centre itself. The instinct to ask “who owns the data centre” collapses several genuinely separate ownership questions into one and in doing so obscures where the real leverage sits. As mentioned earlier, the physical infrastructure (land, building, power connection, cooling plant) is typically owned by a data centre company (NextDC, AirTrunk, Macquarie Data Centres, Firmus, etc.), often Australian-incorporated even when foreign-capitalised. The compute hardware inside (GPUs, servers) may be owned or leased by the tenant, cloud provider or specialist compute provider.

Microsoft’s cloud architecture operates through “regions”. In the corporation’s usage, a region is a specific, customer-selectable geographic deployment location made up of one or more

³⁸ Hawkins Z., Lehdonvirta V. and Wu B. “AI Compute Sovereignty: Infrastructure Control Across Territories, Cloud Providers, and Accelerators”. (June 20, 2025). p. 15. Available at SSRN: <https://ssrn.com/abstract=5312977> or <http://dx.doi.org/10.2139/ssrn.5312977>.

³⁹ Ibid. p. 6.

⁴⁰ Ibid. p. 14.

interconnected physical data centres, nested within a broader "geographical" boundary used for data-residency purposes. Since Australia contains multiple such regions (e.g. "Australia East," "Australia Southeast") nested within a single "Australia" geography, an Australian customer or government agency can choose an in-country region to satisfy data-residency requirements, but that choice governs only where the customer's designated resources are deployed, not necessarily the identity, control-plane, or orchestration systems that continue to operate from, and remain legally reachable via, Microsoft's global infrastructure, largely based in the US. Cross-region replication of data to facilities outside Australia is not automatic by default, but it is readily available and commonly configured for purposes such as disaster recovery, meaning data nominally "resident" in Australia can, depending on the customer's own architectural choices, still be deliberately or incidentally replicated to data centres in other countries.

Box 1: Where does a data centre's data go: the case of Microsoft

What is physically located in Australia: the accelerators themselves (the physical GPU/AI accelerator silicon, racks, power infrastructure, cooling systems). When a workload runs "in" the Australian data centre, the actual computation (electrons switching in the actual chips) genuinely happens on Australian soil, using Australian electricity, generating Australian heat.

What is not confined to Australia

- **Regions are deliberately interconnected by design, not isolated.** The Azure global network backbone connects data centres through Microsoft's global network of "regions".¹ Multi-region architectures are commonly used for resilience, disaster recovery and service availability, although they must be configured accordingly.
- **The compute *decision*, which physical facility executes a given job, depends on how the service is configured.** Load balancing, auto-scaling and traffic-management services (explicitly including Azure Traffic Manager) can direct requests between configured regional endpoints. This does not mean Australian workloads are automatically or routinely processed overseas.
- The broader service architecture is not necessarily confined to Australia, even when computation occurs there. Some identity, management, metadata and orchestration functions may operate across regions or outside Australia, depending on the service and configuration
- **"Location"** is also affected by customer configuration and the service used. Data residency boundaries exist at the Azure geography level and Microsoft advises customers with residency requirements to select regions within the required geography.
- **Cross-region replication for resilience** is supported and commonly used and some Azure services provide built-in cross-region replication and failover. Importantly, Azure region pairs are generally located within the same geography; for example, Australia East is paired with Australia Southeast. Cross-region replication therefore does not necessarily mean data leaves Australia.

The most precise and defensible formulation of where data is located is neither "located in Australia" nor "globally networked" alone. The physical compute substrate is located in Australia, while the system it belongs to may remain part of a globally operated architecture whose broader functions and dependencies vary by service and configuration. "Located in Australia" is true of the hardware in the narrowest physical sense; it does not, by itself, establish Australian ownership, operational control or complete technological independence. Microsoft

does offer Australian data residency options for relevant services, but the applicable guarantees must be assessed service by service.

Beyond the location and movement of data, there are questions of ownership of the data, the software, the physical infrastructure and the data centre itself.

The instinct to ask “who owns the data centre” collapses several genuinely separate ownership questions into one and in doing so obscures where the real leverage sits. The physical infrastructure (land, building, power connection, cooling plant) is typically owned by a data centre company (NextDC, AirTrunk, Macquarie Data Centres, Firmus, etc.), often Australian-incorporated even when foreign-capitalised. The compute hardware inside (GPUs, servers) may be owned or leased by the tenant, cloud provider or specialist compute provider.

The software (the model weights, training code, inference stack) may be owned or licensed by the AI or software provider, irrespective of whether it runs on Australian infrastructure. And the data being processed (training materials, customer inputs, outputs) has its own separate ownership and rights chain, frequently belonging to neither the data centre operator nor the AI company but to the original rights-holders or data subjects. The practical upshot is that answering the question about “who owns the data centre” tells you relatively little about who ultimately controls the AI activity occurring within it. A wholly Australian-owned building can host foreign-owned or controlled compute models, while rights in the data may sit with multiple other parties. Each of those layers can be transferred, sold, or restructured independently of the others. Ownership at the level of bricks and land is therefore not, by itself, a reliable proxy for technological strategic control. These are familiar issues that have been discussed extensively in the context of cloud computing.

Who governs it? This is better understood in granular terms as “who governs it and by what means”.

Australian law already captures important elements of ownership, security and control through mechanisms including foreign investment review and, for qualifying critical data storage or processing assets, obligations under the Security of Critical Infrastructure Act 2018 (SOCI Act).⁴¹ The Government’s proposed national data-centre standards would add further requirements relating to matters including energy and water. These mechanisms do not, however, answer every question of operational or technological control.

A foreign AI company that is the anchor tenant underwriting a data centre’s construction may exercise substantial commercial influence over that site’s future even without owning the land. It can dictate technical specifications, security architecture, staffing access and future demand for capacity. These considerations may also shape the operator’s infrastructure requirements and indirectly demand on Australian energy and planning systems.

Chip suppliers like Nvidia can exercise significant influence through the availability and allocation of advanced accelerators, while foreign governments can separately affect access through export-control regimes applying to advanced chips or AI technologies. These dependencies mean decisions made outside Australia can affect the technologies Australian operators are able to procure or deploy.

⁴¹ Australia. Cyber and Infrastructure Security Centre, Department of Home Affairs (Australia). “SOCI Act 2018 for Data Storage and Processing.” Canberra: last updated 5 December 2023. <https://www.cisc.gov.au/information-for-your-industry/data-storage-and-processing/legislation-regulation-and-compliance/soci-act-2018>.

Cloud and AI companies also retain remote administrative control through software updates, security monitoring, service configuration and model deployment over infrastructure and workloads physically located in Australia. These forms of operational control continue after planning and investment approvals have been granted.

Even if every formal ownership and approval box is ticked according to Australian law, technical, contractual and supply-chain dependencies may therefore remain strategically significant. The relevant governance analysis should consider not only formal ownership and legal jurisdiction, but who can control access to compute, modify the technology being operated, supply critical components and determine whether services continue to be available.

Recommendations

Australia does not need to choose between technological capability and community protection, geopolitical resilience, or national policy capacity. It should pursue them all. Government has already committed to an enforceable social licence for AI infrastructure. The recommendations below set out what that commitment requires in practice, organised into two linked sets that correspond to the questions this submission has addressed: **(A)** an enforceable social licence for the communities hosting data centres and **(B)** the strategic and geopolitical governance capability Australia needs to manage the layered ownership and diffuse control such facilities involve. A shared design principle runs through both clusters and is stated once here rather than repeated: wherever this submission recommends approval conditions, standards, or licences, they should operate as ongoing obligations, subject to audit, monitoring and proportionate enforcement throughout the life of the asset.

Set A: An enforceable social licence for host communities

Essential

A legislated national minimum standard.

Major facilities should be subject to statutory requirements — not departmental "expectations" — covering community participation, electricity, water, emissions, thermal effects, cumulative impacts, siting, monitoring and public reporting, with legislation identifying the Commonwealth authority responsible for enforcement and its interaction with state and territory regulators. States and territories should remain free to impose stronger requirements, but the Commonwealth standard should set an enforceable floor. Compliance should be ongoing rather than assessed only at commissioning, with proportionate consequences available for material or repeated breach.

Mandatory early consultation.

This should be triggered before location, energy supply and core design decisions become effectively irreversible, with the trigger point defined in legislation or regulation and occurring before material site, grid-connection or design commitments are finalised, rather than left to developer discretion.

A designated accountable decision-maker.

This authority should be designated in legislation rather than described generically, so communities know which specific authority is responsible for evaluating their concerns and certifying that consultation requirements have been satisfied — with that authority's decisions subject to independent review.

A genuine causer-pays principle, applied as a default rule rather than a disclosure requirement. Additional electricity, network, water, monitoring and mitigation costs created by private infrastructure should be borne by developers and operators as a condition of approval; any exception allowing cost transfer to households or taxpayers should require explicit, published, time-limited justification. This would build on the Government's existing expectation that data centres cover their share of transmission, distribution and water-infrastructure costs.

Clear, tiered consequences for non-compliance.

Failure to complete mandatory consultation or required impact assessments should prevent an application progressing until deficiencies are remedied. Materially false or misleading disclosures should attract existing or enhanced penalties. Serious or repeated breaches of community-protection conditions should trigger escalating consequences under the applicable statutory regime, including supervision where authorised by law.

Supporting mechanisms

Mandatory cumulative precinct assessment.

Applying the Lane Cove evidence set out above: existing, approved and reasonably foreseeable data centres should be assessed together wherever they share local electricity, water, transport, environmental or residential systems.

Population exposure assessment.

ABS data should be integrated with site-specific thermal, acoustic and air-dispersion modelling to identify the number of residents and sensitive receptors within predicted impact areas, before approval.

Independent baseline and continuing monitoring.

Relevant air pollutants, environmental noise, temperature, water use and backup-generation operation should be independently monitored, at the developer's cost and results published in a standard, comparable format across facilities.

A statutory Community Response Statement.

Material issues raised through consultation should be documented alongside the evidence considered, project changes made, concerns not accepted and reasons for those decisions, thereby providing the public record against which the accountable decision-maker and the non-compliance regime can be tested.

Set B. Strategic and geopolitical governance capability

Given the layered ownership and diffuse governance described above, the sensible response is not to chase clean ownership rules which industry can always restructure around but to build durable, adaptive levers at the points where Australia can exercise control: policy expertise, energy, data, contracts and standards.

Invest in AI policy expertise well beyond current levels.

Australia should build a standing, well-resourced AI policy capability with several competing centres of analysis addressing technical, legal, economic, social and strategic considerations in a multi-disciplinary manner, networked across government, universities, industry and civil society while preserving independent analysis. Australia's AI Safety Institute has a distinct remit focused on AI capabilities, risks, harms and safety; it should be complemented by broader geopolitical, economic, infrastructure and social-policy expertise. The capability should be robustly networked into Europe, Japan, South Korea, Singapore and Taiwan. Without deeper capability, Australia risks negotiating major long-term technology and infrastructure arrangements without sufficient independent analytical capacity.

Build public equity or co-investment stakes into strategically significant projects.

The Australian government could consider extending existing Australian Industry Participation approaches for major projects to the AI infrastructure sector. Australia already requires qualifying projects of \$500 million or more to provide Australian businesses with full, fair and reasonable opportunities to participate. For example, Australia could require foreign investors in large data-centre projects to fund, on an untied basis, a significant expansion of AI research and education activity, nationally or locally. Related proposals, such as equity stakes, a compute reserve and public-sector access rights, as advocated by Dr Raffaele Ciriello,⁴² are worth considering. These options could give Australia influence over strategically significant infrastructure beyond initial planning approval and increase the proportion of public value retained domestically.

Diversify supply-chain and jurisdictional dependency rather than trying to eliminate it.

Since chip allocation, export controls and remote software governance sit largely outside Australian law, the more realistic goal is redundancy: encouraging multiple hardware suppliers and multiple AI-company tenants across the data-centre estate, rather than concentration on one or two foreign firms whose home-government decisions could unilaterally affect Australian capacity — including diversifying toward the European Union as a supplier of AI investment and technology.

Separate and regulate the four ownership layers explicitly.

Because infrastructure, hardware, software and data have different owners, different risk profiles and different legitimate levers of control, policy should name each layer separately: critical-infrastructure rules for the physical site where the SOCI Act applies; residency and privacy requirements for the data layer; security and access controls for remote software administration; and content/copyright licensing regimes for training inputs. Bundling all four into a single "data centre" policy conversation weakens national control while treating them as four distinct regulatory objects can strengthen national control.

⁴² Ciriello, Raffaele F. "To Avoid US-Style AI Backlash, Australian Data Centres Need Collective Sovereignty, Not Corporate Extraction." *Australian Outlook*, Australian Institute of International Affairs, 25 June 2026, <https://www.internationalaffairs.org.au/australianoutlook/to-avoid-us-style-ai-backlash-australian-data-centres-need-collective-sovereignty-not-corporate-extraction/>.

References

- Albanese, Anthony (Prime Minister of Australia). "AI: Australia's Interests" (media statement), 15 July 2026, <https://www.pm.gov.au/media/ai-australias-interests>
- Austin G, Bappanad K, Henry A, Materano L, Michael K, Reddy B, Walker-Munro B, Withers G: "Key Dimensions in Technology Impact Assessment for Peace and Stability: Australia and India," in *IEEE Transactions on Technology and Society*, 2026, doi: 10.1109/TTS.2026.3718558.
- Australia. Cyber and Infrastructure Security Centre. Department of Home Affairs. "SOCI Act 2018 for Data Storage and Processing." Canberra: last updated 5 December 2023. <https://www.cisc.gov.au/information-for-your-industry/data-storage-and-processing/legislation-regulation-and-compliance/soci-act-2018>
- Australia. Department of Foreign Affairs and Trade. "Climate Change and Resilience." Canberra: Australian Government. <https://www.dfat.gov.au/geo/pacific/development-assistance/climate-change-and-resilience>
- Australia. Department of Industry, Science and Resources. "Expectations of Data Centres and AI Infrastructure Developers," 23 March 2026, <https://www.industry.gov.au/NationalDataCentreExpectations>
- Australia. Department of Industry, Science and Resources. National AI Plan, 2 December 2025, <https://www.industry.gov.au/publications/national-ai-plan>
- Australia. Senate Environment, Communications, Information Technology and the Arts References Committee. Commonwealth Environment Powers Inquiry, 1999, https://parlinfo.aph.gov.au/parlInfo/download/publications/tables/papers/8725/upload_pdf/HPP042016001176.pdf
- Australia. Senate Environment and Communications References Committee. Parliamentary Inquiry into Artificial Intelligence and Data Centres (terms of reference), 2026. https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/Aldatacentres48P
- Australia. Prime Minister of Australia. "Statement following the meeting of National Cabinet". 26 August 2026. <https://www.pm.gov.au/media/meeting-national-cabinet-26-august-26>.
- Australian Government and Anthropic. Memorandum of Understanding between the Australian Government and Anthropic on Collaboration on AI Opportunities, 1 April 2026, <https://industry.gov.au/publications/memorandum-understanding-between-australian-government-and-anthropic-collaboration-ai-opportunities>
- Barracough, Ashleigh. "Firmus 288-Megawatt AI Data Centre at Bell Bay, Tasmania Gets Approval After 6-1 Council Vote." *ABC News*, 26 August 2026. <https://www.abc.net.au/news/2026-08-25/firmus-ai-bell-bay-receives-george-town-council-approval/107074336>
- Bouchard, N. "The AI Sovereignty Paradox: France and the Limits of Digital Autonomy", Social Cyber Institute, August 2026, in publication.
- Ciriello, Raffaele F. "To Avoid US-Style AI Backlash, Australian Data Centres Need Collective Sovereignty, Not Corporate Extraction." *Australian Outlook*, Australian Institute of International Affairs, 25 June 2026, <https://www.internationalaffairs.org.au/australianoutlook/to-avoid-us-style-ai-backlash-australian-data-centres-need-collective-sovereignty-not-corporate-extraction/>
- CBC News. "AI Data Centre Opposition, Explained" (reporting Angus Reid Institute survey, June 2026), <https://www.cbc.ca/news/canada/ai-data-centre-opposition-explained-9.7225796>

- DigNetSol. "Sustainability Tech: AI Data Centres May Heat Surrounding Areas for Miles," 2026 (preprint, not yet peer-reviewed), <https://dignetsol.co.uk/news-resources/sustainability-tech-ai-datacentres-may-heat-surrounding-areas-miles>
- Environmental Defenders Office (EDO). Summary of UN General Assembly Resolution 76/300: The Human Right to a Clean, Healthy and Sustainable Environment, August 2022, https://www.edo.org.au/wp-content/uploads/2022/08/EDO_HealthyEnvironment_Summary_Web.pdf
- Goodman Group. "Project Mars, 12 Mars Road" (project documentation), 2026, <https://au.goodman.com/property-lease-site/project-mars>
- Hawkins Z., Lehdonvirta V. and Wu B. "AI Compute Sovereignty: Infrastructure Control Across Territories, Cloud Providers, and Accelerators". (June 20, 2025). p. 15, Available at SSRN: <https://ssrn.com/abstract=5312977> or <http://dx.doi.org/10.2139/ssrn.5312977>.
- Jones, Jeffrey M. "Americans Oppose AI Data Centers in Their Area." *Gallup News*. 13 May 2026. <https://news.gallup.com/poll/709772/americans-oppose-data-centers-area.aspx>
- Lane Cove Council. "Have Your Say: Data Centre Proposed for 12 Mars Road". 21 April 2026. <https://www.lanecove.nsw.gov.au/Council-News/Have-Your-Say-Data-Centre-Proposed-for-12-Mars-Road>
- Lane Cove Council. "Major Projects Council Submission Project Mars Data Centre (SSD-82052708) (Lane Cove)". 20 April 2026. <https://ecouncil.lanecove.nsw.gov.au/trim/DocumentLink.asp?RecId=28938/26>
- Reuters. "Anthropic Says AI Labs Need Coordinated Plan to Halt Development if Risks Rise," 4 June 2026, <https://www.reuters.com/business/anthropic-says-ai-labs-need-coordinated-plan-halt-development-if-risks-rise-2026-06-04/>
- Sailor, D. J., Abolhassani, S. S., and Martin, E. P. "Data Center Waste Heat as an Emerging Urban [Environmental Effect]." *Journal of Engineering for Sustainable Buildings and Cities* (ASME), vol. 7, no. 2, art. 024501, 2026, <https://asmedigitalcollection.asme.org/sustainablebuildings/article/7/2/024501/1233035/Data-Center-Waste-Heat-as-an-Emerging-Urban>
- Science Direct. "Heat Rejection" (topic overview), <https://www.sciencedirect.com/topics/engineering/heat-rejection>
- Social Cyber Institute. "Technology Impact Assessment for Peace and Stability: A Comparative Study on Australia and India", June 2025, p. ii, https://www.socialcyber.co/_files/ugd/15144d_c5acc66a4a014035a939a1b534f06822.pdf
- Svantesson D. "A Starting Point for Re-thinking 'Sovereignty' for the Online Environment." In *Data Sovereignty: From the Digital Silk Road to the Return of the State*, edited by Anupam Chander and Haochen Sun. New York: Oxford Academic, online edn, 14 December 2023. <https://doi.org/10.1093/oso/9780197582794.003.0003>
- United States. Census Bureau. Geography Program Glossary. "Census tracts". https://www.census.gov/programs-surveys/geography/about/glossary.html#par_textimage_13