



Government Administration Committee A
Inquiry on AI Data Centres in Tasmania

The House of Assembly Standing Committee on Government Administration A has resolved to inquire into and report upon the construction and operation of AI data centres in Tasmania.

Members of the public may use this form as a template to provide comment on the Committee Inquiry Terms of Reference. The Terms of Reference are set out below and comments should be limited to these areas.

Submissions become Committee documents that may be published on the Committee website and quoted in the Committee's report to Parliament. Should you not wish whole or parts of your submission to be published, please clearly indicate this in your submission. Persons making submissions must not release them without the approval of the Committee. Submissions are protected by parliamentary privilege but the unauthorised release of them is not.

Submissions should be received by the closing date of **Monday, 21 September 2026** and should be emailed to assemblygaa@parliament.tas.gov.au, or posted to: Secretary, Inquiry into AI Data Centres in Tasmania, Parliament House Hobart, 7000.

Submitters contact details:

Name: Denise King

Email: [REDACTED]

Contact number: [REDACTED]

Terms of Reference:

Inquire into and report upon the construction and operation of AI data centres in Tasmania, including recommending future legislation and regulations necessary to:

1. Protect public resources and the environment;

AI data centres require substantial quantities of electricity and, depending on the technology used, significant quantities of water.

Electricity requirements should be considered in the context of Tasmania's existing electricity generation, transmission capacity, expansion of the AI Data Centres due to technology upgrades and reliability. Where a new data centre creates substantial additional electricity demand, there should be a clear requirement for the proponent to demonstrate how that additional demand will be met without compromising the reliability or affordability of electricity for the Tasmanian community.

Where additional renewable generation is proposed to support a data centre, there should be clear and measurable commitments regarding the amount, timing and delivery of that generation. These commitments should be established before, or progressively in parallel with, the operation of the facility rather than relying solely on broad future intentions.

Emergency diesel or other fossil-fuel generators are proposed in planning documents to provide the necessary power in case of network failures. However, their use should be tightly regulated, monitored and reported so that emergency generation does not become a routine source of electricity.

Water is another important issue. Water availability varies significantly between locations, and Tasmania's water resources cannot be treated as an unlimited resource. Regulations should establish appropriate benchmarks for water consumption and require proponents to demonstrate that their water requirements will not cause unacceptable impacts on local communities, agriculture, industry, waterways or the environment. Even going as far as demanding that AI Data centres transition to using desalination water so as not to impact on fresh water supplies.

Water consumption, sources, discharge and any reliance on potable water should be transparently reported.

2. Ensure Tasmania's Resource Management and Planning System adequately recognises and addresses the specific impacts of the development and construction of AI and data facilities;

Data centres should generally be located in areas appropriately zoned for large-scale industrial infrastructure and where the surrounding infrastructure is capable of supporting the proposed development. Particular consideration should be given to the proximity of residential areas, schools and other sensitive land uses, including those areas that are near conservation areas that support critically endangered species habitat.

Noise (including low noise frequency) and light pollution require proper assessment, including the cumulative effect of industrial facilities operating continuously, including throughout the night. Assessments should not focus only on average noise levels if there are potential low-frequency, tonal or intermittent noise impacts that may be experienced differently by nearby residents.

Planning assessments should also consider the cumulative impacts of multiple industrial facilities rather than assessing each proposal in isolation.

Before approval, proponents should be required to provide clear, independently verifiable information concerning:

- electricity demand;
- water demand and source;
- wastewater and discharge;
- backup generation;
- noise and low-frequency noise;
- light pollution;
- electromagnetic infrastructure where relevant;
- environmental impacts;
- traffic and infrastructure requirements; and
- the expected operational characteristics of the facility.

3. Provide Parliamentary oversight and accountability for new facility construction and resource allocation;

Given the fast paced demand, scale and strategic importance of AI infrastructure, significant data centre developments should be subject to appropriate Parliamentary and regulatory oversight. There should be transparent reporting of commitments made by proponents concerning the additional cost of electricity (including network transmissions), water, renewable energy, employment, environmental management (including protecting agricultural land, wildlife with an emphasis of endangered species) and community benefits. Commercial confidentiality should not be applied so broadly that the community is prevented from understanding the significant cost to upgrade the use of public infrastructure or resources to power these AI Data Centres.

There is also an important distinction between the physical infrastructure and the technology that operates through it. While planning authorities should assess the physical impacts of data centres, the Commonwealth should ensure that AI applications involving personal information, surveillance, facial recognition, biometric identification and automated decision-making are subject to appropriate national regulation.

Protection of biometric information

AI systems increasingly have the capacity to identify or analyse people through their faces, voices, fingerprints, iris patterns, gait and other characteristics. Biometric information is fundamentally different from an ordinary password or identification number because an individual cannot simply replace their face, fingerprints or voice if that information is compromised.

The use of AI infrastructure should therefore not create an environment in which biometric information can be collected, analysed, retained or shared without strong safeguards.

4. Ensure transparent public disclosure of resource consumption;

Transparency is essential if the Tasmanian community is to make informed judgements about AI data centres.

Proponents should be required to publicly report, in an accessible and understandable form:

- electricity consumption and how will it impact on household demand;
- water consumption;
- the source of water with the need to invest in the use of desalination water;
- wastewater and environmental discharge;
- renewable electricity generated or contracted who has ownership and how does it provide investment to the Tasmanian population;
- use of backup generators;
- significant environmental incidents;
- noise monitoring results where relevant; and
- material changes to the facility's operation.

Information should not be withheld merely by broadly referring to commercial confidentiality where the information concerns the use of public resources or infrastructure.

The community should be able to understand the actual resources being consumed and the infrastructure being provided or upgraded to support a facility.

5. Provide the Tasmanian community with adequate opportunities for consultation;

Meaningful consultation requires more than providing large quantities of technical documentation shortly before a decision is required.

Information about proposed data centres should be presented in a form that ordinary members of the community can understand. Independent assessment is particularly important where proponents provide highly technical information about electricity, water, noise, environmental impacts or emerging technology.

The community should have sufficient time to consider the proposal, obtain independent advice and provide informed submissions.

The consultation process should also recognise that AI data centres involve both physical infrastructure and emerging technologies that will expand rapidly as technology advances. Community concerns about the future use of AI, including facial recognition and biometric surveillance, should not simply be dismissed as unrelated to the development of the infrastructure that makes large-scale AI applications possible.

6. Ensures the Tasmanian community receive tangible benefits from all AI and data facilities constructed in the state; and

AI data centres have the potential to provide employment, construction activity, technical training and opportunities for Tasmanian businesses.

However, expectations about employment should be realistic. Increasing automation and efficiency may mean that highly capital-intensive facilities do not provide employment on the scale historically associated with large industrial projects.

Benefits should therefore include consideration of:

- Tasmanian employment;
- apprenticeships and training;
- technology and engineering skills development;
- opportunities for Tasmanian businesses;
- investment in local infrastructure where appropriate; and
- long-term skills development that enables Tasmanians to participate in the technology sector.

Any public subsidies, concessions or preferential access to resources should be transparent and demonstrably provide an appropriate public benefit.

7. Any other matter incidental.

The Committee should also consider the rapidly developing ability of AI systems to use a person's photograph, facial characteristics or voice to create material that the person did not create and has not consented to.

AI applications are now capable of taking an ordinary photograph of a person and manipulating or combining it with other material to create highly realistic images, including sexually explicit or otherwise inappropriate images. This creates a significant privacy and personal-safety risk because the victim may have done nothing more than have their photograph publicly available or provide an image for an entirely legitimate purpose.

The same concern applies to **voice cloning**. AI systems can increasingly reproduce a person's voice from recordings and generate new speech that can sound convincingly like the individual. This creates risks of impersonation, fraud, harassment, reputational damage and the creation of recordings that appear to show a person saying something they never said. Canada's federal privacy authority has specifically identified the risks associated with deepfakes, voice synthesis and other impersonation technologies using biometric information.

These technologies demonstrate why biometric information requires stronger protection than an ordinary piece of personal information. A password can be changed after a security breach. A person's face, fingerprints, distinctive physical characteristics or voice cannot simply be replaced. Once biometric information has been copied, used to create a synthetic identity or incorporated into an AI system, the consequences may be extremely difficult to reverse.

The Committee should therefore consider whether Tasmania's existing legal and regulatory framework provides adequate protection for biometric information in an environment where AI can transform photographs, facial characteristics and voice recordings into new synthetic material.

International regulatory developments

Tasmania should also examine developments in other jurisdictions rather than assuming that existing privacy protections will remain adequate as AI capabilities develop.

The European Union has introduced specific AI rules addressing the generation of non-consensual sexually explicit and intimate material, including AI "nudification" applications. The EU's regulatory framework also establishes transparency obligations for certain AI-generated or manipulated content, including deepfakes, and provides specific regulation for high-risk AI applications involving biometrics.

European legislation addressing violence against women also specifically recognises the non-consensual production or manipulation of sexually explicit material using artificial intelligence, including deepfakes that falsely make it appear that an identifiable person is engaged in sexual activity.

Canada's privacy authorities have similarly recognised that biometric information is particularly sensitive because it is unique to an individual and difficult to change. Canadian privacy guidance identifies the risks associated with facial recognition, deepfakes, voice synthesis and other forms of biometric impersonation.

These international developments provide an important warning for Tasmania: the legal protection of biometric information needs to anticipate what AI can do with that information, not simply regulate the original collection of the photograph, recording or biometric identifier.

Recommended safeguards

The Tasmanian Government should consider establishing clear requirements for AI systems and organisations that collect, process or retain biometric information, including:

- a clearly defined and lawful purpose for collecting biometric information;
- meaningful consent where consent is the appropriate legal basis;
- strict limits on using photographs, facial information or voice recordings for unrelated AI training or commercial purposes;
- privacy impact assessments for high-risk biometric AI applications;
- strong security requirements and independent auditing;
- strict retention and deletion requirements;
- restrictions on secondary use, sale or disclosure of biometric information;
- clear notification when AI-generated or manipulated material is being presented as authentic;
- mechanisms for individuals to report, remove and seek remedies for non-consensual AI-generated material;
- safeguards against AI systems being used to create non-consensual sexualised images or impersonate individuals through cloned voices;
- clear legal responsibility for organisations that negligently allow their AI systems to be used for these purposes; and
- consideration of whether individuals should have specific rights concerning the use of their likeness, face and voice by AI systems.

A particularly important principle should be that consent to provide a photograph or voice recording for one purpose should not automatically constitute consent for that material to be used to train AI, create a digital likeness, generate synthetic images, clone a person's voice or produce other biometric representations.

The Committee should also consider the potential cross-border nature of these harms. An image or voice may be collected in Tasmania, processed by an overseas AI provider, stored in another country and then distributed globally. Tasmanian protections therefore need to consider not only where the original data was collected and stored but also what can subsequently be done with it.

The fundamental issue is simple: people should retain meaningful control over their identity, likeness and voice in an age where AI can reproduce them without their participation.

A further issue requiring consideration is the rapid expansion of AI-enabled surveillance and biometric technology.

Tasmania should therefore ensure that the development of AI infrastructure occurs alongside appropriate safeguards for individual privacy and civil liberties.

In particular, the Tasmanian Government should advocate to the Commonwealth for a strong and nationally consistent framework governing biometric information, facial recognition and other AI-enabled identification technologies.

The framework should recognise that biometric information is particularly sensitive because it is intrinsically connected to an individual and generally cannot be changed if compromised.

The collection of biometric information should therefore be subject to necessity, proportionality, transparency, security, retention and purpose-limitation requirements.

AI systems should not be permitted to expand their use of biometric information simply because the technological capability exists. The existence of a technical capability to collect, analyse or identify individuals does not, by itself, establish that the collection is necessary or appropriate.

Independent oversight is particularly important where biometric systems could affect a person's access to services, employment, education, security, law enforcement or other significant aspects of their life.

Conclusion

Tasmania should not be required to choose between technological development and the protection of its people, resources, businesses and environment. However, neither should Tasmania assume that a large private investment automatically represents a net public benefit.

The appropriate question is whether the total benefits exceed the total costs, including costs that may not appear on the proponent's balance sheet. Those costs include electricity generation and transmission infrastructure, water infrastructure, roads and other public infrastructure, government resources, environmental impacts, resource opportunity costs and any costs that may ultimately be borne by households or existing Tasmanian businesses.

Most importantly, the assessment must consider what Tasmania is giving up or additional costs to their utility bills in order to accommodate the development.

Electricity, fresh drinking water, land (in particular agricultural land), infrastructure capacity and public expenditure are finite resources. Allocating substantial quantities of those resources to one new industry can affect the capacity of existing industries and businesses to expand and can influence Tasmania's future economic choices. That is why the Committee should require a transparent assessment of both the private economic benefit and the public economic cost of major AI data centres.

The same principle should apply to personal information. AI infrastructure should not develop faster than the safeguards protecting Tasmanians from inappropriate collection, processing and use of their personal and biometric information. Tasmania has an opportunity to establish these safeguards now. The objective should be responsible investment, not investment at any cost.

The test should be whether an AI data centre provides a genuine, demonstrable and lasting net benefit to Tasmania after the full infrastructure, resource, economic, environmental and community costs have been taken into account.

