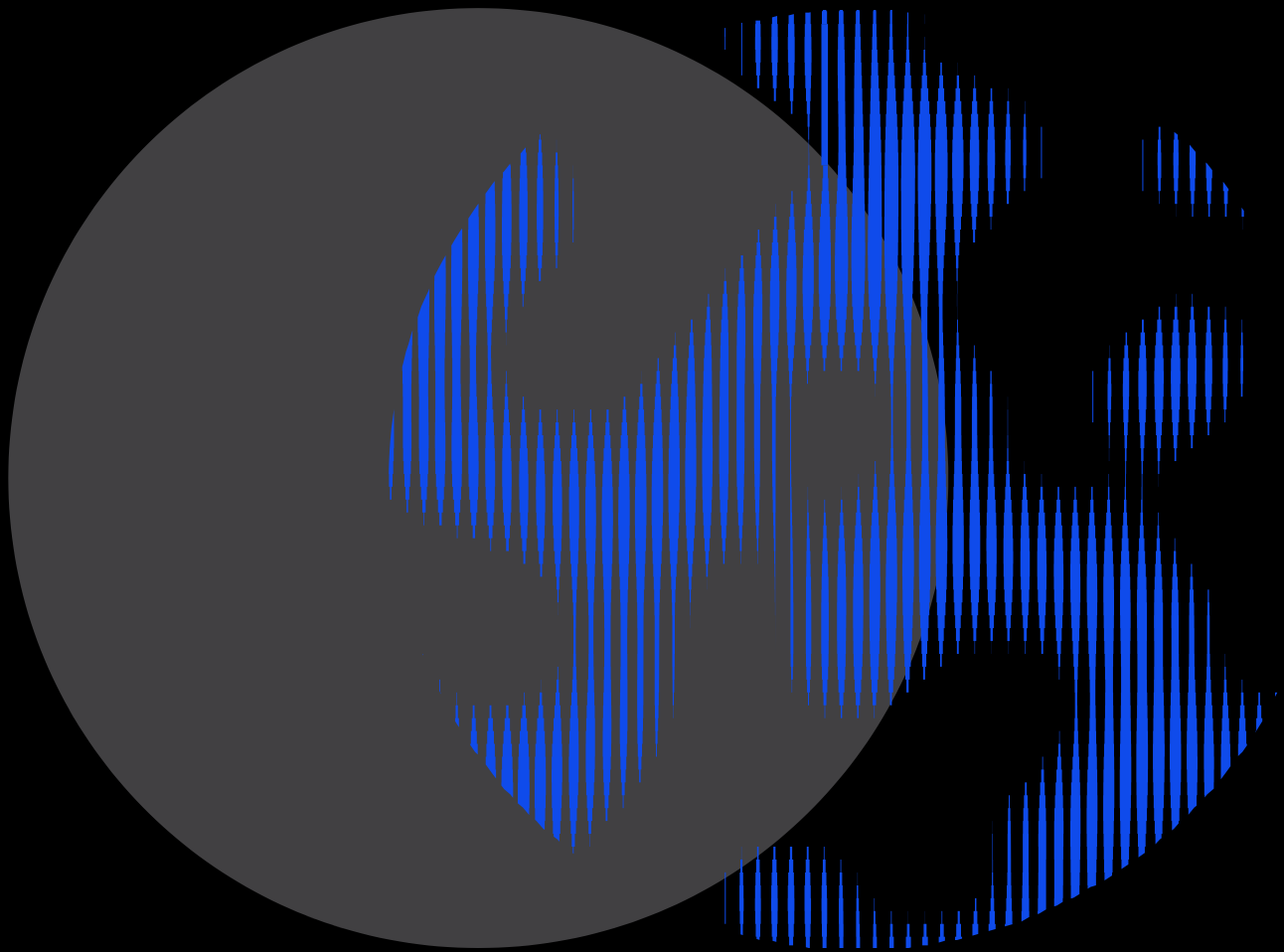




**Human Technology
Institute**



Inquiry into Artificial Intelligence

Submission to the Joint Select Committee on Artificial Intelligence

14 September 2026

The Human Technology Institute (HTI) is building a future that applies human values to new technology. HTI embodies the strategic vision of the University of Technology Sydney (UTS) to be a leading public university of technology, recognised for its global impact specifically in the responsible development, use and regulation of technology. HTI is an authoritative voice in Australia and internationally on human-centred technology. HTI works with communities and organisations to develop skills, tools and policy that ensure new and emerging technologies are safe, fair and inclusive and do not replicate and entrench existing inequalities. The work of HTI is informed by a multi-disciplinary approach with expertise in data science, law and governance, policy and human rights.

For more information, contact us at hti@uts.edu.au

Authors: Clare Brennan, Jenna Hand, Lauren Perry, Sarah Sacher, and Prof Edward Santow

Acknowledgement of Country

UTS acknowledges the Gadigal people of the Eora Nation, the Boorooberongal people of the Dharug Nation, the Bidiagal people and the Gamaygal people upon whose ancestral lands our university stands. We would also like to pay respect to the Elders both past and present, acknowledging them as the traditional custodians of knowledge for these lands.

Table of contents

Table of contents 3

Executive summary 4

List of recommendations 5

Transparency for data used to train AI models..... 6

Targeted reform to address tech-enabled worker surveillance 8

Law to govern automated decision making 11

Modernising Australian privacy law 14

Appendix A 17

Appendix B 18

Endnotes..... 25

Executive summary

The UTS Human Technology Institute (HTI) welcomes the opportunity to contribute to the inquiry of the Joint Select Committee on Artificial Intelligence (the Committee).

Artificial intelligence (AI) has the potential to drive economic growth, innovation and productivity. It also carries significant risks to people and the systems and institutions we rely on. The National AI Plan commits the Government to ensure Australians share in the benefits of AI while remaining protected from its potential harms.

And yet Australians have very low trust in AI: only 30% of Australians believe the benefits of AI outweigh the risks, the lowest ranking globally.¹ The Government has rightly identified community trust in AI as vital to our country's technological future, with senior ministers saying, "Countries that get AI safety right will be those building the trust needed for people and businesses to confidently adopt and embrace the benefits of AI".²

This submission responds to paragraph 1(i) of the terms of reference: "the adequacy of Australia's existing laws and regulatory frameworks as they apply to AI and whether there are any gaps that warrant reform".³ We focus on four key areas of reform where timely action by government is needed to build a firm foundation of community trust in AI, so as to address more effectively the risks and opportunities that AI brings.

Each of these reforms is urgent, important and practically achievable in a short period:

- **Transparency for data used to train AI models.** The Government is currently developing Australian Standards for AI to promote training of AI models onshore in ways that bring benefits to Australia and address community concerns regarding energy, water and more broadly. HTI proposes that these Standards should include a training data transparency requirement, modelled on similar laws already operating in jurisdictions like California. Such a transparency requirement would support the upholding of copyright, privacy and other laws. It would also allow Australians to make more informed choices about which AI models to use.
- **Targeted reform to address tech-enabled worker surveillance.** HTI proposes some straightforward amendments to the Fair Work Act to give employers clarity on how they can safely and reasonably monitor their works, and to protect those workers against harmful surveillance in the workplace. This is an increasingly urgent issue: while just 9% of Australian employees surveyed in 2026 believe they are monitored in their own workplace,⁴ 91 percent of Australian employers surveyed in 2021 reported monitoring their remote workers' locations through software.⁵
- **Law to govern automated decision making.** The Government has committed to implement the 2023 Robodebt Royal Commission recommendation to legislate a framework for automated decision making (ADM) in government services. As government increases its use of ADM, this proposed law must give clarity for agencies in how they should develop ADM systems, while providing clear

protections against risks and harms associated with ADM. An ADM law cannot be judged merely on whether it facilitates ADM by government, it must also ensure that such decision making is accurate, fair lawful and accountable.

- **Modernising Australian privacy law.** Australians rate protection of personal privacy as their top priority for AI regulation.⁶ HTI supports the Exposure Draft Privacy Amendment (Personal Data Protection) Bill 2026, subject to some amendments outlined below. This once-in-a-generation reform would bring our privacy law into the AI era, and give greater confidence that this technology will not be used to exploit and harm Australians.

List of recommendations

Transparency for data used to train AI models

1. The Australian Government should include a training-data transparency requirement in the Australian Standards for AI, which are currently being developed. In developing this requirement, the Government should provide an opportunity for public input via its upcoming public consultation process on the Standards.

Targeted reform to address tech-enabled worker surveillance

2. The Australian Government should lead national worker surveillance reform by:
 - a) introducing a requirement in the Fair Work Act that any worker monitoring be 'fair and reasonable' outlining the relevant factors that apply to this context
 - b) establishing a dedicated complaints stream in the Fair Work Commission to hear privacy-related worker complaints
 - c) amending the Fair Work Act to ensure that enterprise bargaining agreements and Modern Awards can build on the protections in the proposed 'fair and reasonable' requirement
 - d) supporting regulators such as the Fair Work Ombudsman to issue practical guidance on how to apply new and existing laws in the worker surveillance context.

Law to govern automated decision making

3. The Australian Government should fulfill its commitment to implement recommendation 17 of the Robodebt Royal Commission by introducing a Bill to regulate automated decision making in government. The Bill should contain the necessary safeguards to ensure that ADM operates effectively, lawfully and accountably by requiring:
 - a) Parliament, not a minister or unelected official, to determine when it is appropriate to automate a category of government decision making
 - b) that decisions involving discretion or evaluative judgment generally should not be automated

- c) anyone affected by an automated decision should be given reasons for the decision, and be able to seek effective review of that decision
- d) proactive consideration of the human rights of people likely to be affected by automating a category of decision making before this is permitted.

Modernising Australian privacy law

4. The exposure draft of the Privacy Amendment (Personal Data Protection) Bill 2026 should be passed with HTI's proposed amendments (see Appendix B) to ensure that the reform makes good on the Australian Government's prior commitments to privacy law reform.
5. The Australian Government should further amend the Privacy Amendment (Personal Data Protection) Bill 2026 to include:
 - a) a requirement that the Privacy Commissioner develop a code on biometric and other surveillance technologies, modelled on s 26GC in the current Privacy Act
 - b) a direct right of action where a regulated entity breaches the Australian Privacy Principles.
6. The Australian Government should implement outstanding privacy reform commitments prior to the next Federal election.
7. The Australian Government should make provision to resource the OAIC adequately to ensure that new and existing privacy protections are appropriately understood and enforced.

HTI will make a submission to the Attorney-General's Department with a more detailed articulation of the implications of the Exposure Draft provisions, and our recommended amendments.

Transparency for data used to train AI models

HTI welcomes the Prime Minister's announcement that the Government is developing Australian Standards for AI (the Standards); a legislated national framework covering large data centres and AI training. The Standards have the potential to support the growth of frontier AI training and use in Australia, while protecting the Australian community from some critical risks and harms.

Federal, state and territory governments have publicly recognised the extraordinary energy and water demands of data centres. Less attention has been given to the way the training of AI models – in data centres – uses vast quantities of data. To achieve the Prime Minister's goal, the Standards will also need to give clarity to AI companies regarding their obligations under Australian law, and provide a basis for Australian companies and the broader community to have confidence that laws, including copyright and privacy protections, will be upheld. Protections associated with AI training are particularly relevant because it is during training that decisions are made about the data, content and safeguards that shape model behaviour.

Including a training data transparency (TDT) requirement in the Standards could play a key role in building community confidence in the opportunities associated with growing

this part of the AI industry in Australia, without placing undue additional regulatory burden on AI companies. A TDT requirement would require companies to publish a high-level summary of the data used for training an AI model when it is made available in Australia. Leading companies, including OpenAI and Anthropic, are already complying with TDT requirements in some leading jurisdictions, especially California and the European Union.

A TDT requirement could bring two particular benefits. First, it could enable oversight and appropriate transparency over AI training taking place in Australia, assuring compliance with Australian laws, including copyright law, privacy law, and legal protections against the use of child and sexual abuse material. Second, it could enable the public to make more informed choices about AI models based on information about data inputs and processing.

By way of practical example, a TDT requirement could enable an author of copyrighted books to understand the steps taken by a company engaged in AI training to uphold Australian copyright law, and the major websites used as sources of data for that company's AI training. More broadly, TDT disclosures made by AI companies could allow companies (for example, Canstar), which specialise in helping consumers and companies choose between different product offerings, to rank the various AI models based on their data transparency or legal compliance (similar to those created by the AI Accountability Lab).⁷ A TDT requirement could also encourage companies to keep records of major datasets used for training, and to put in place and track compliance with relevant policies throughout the training process, including copyright and privacy policies.⁸

Including a TDT requirement in the Standards would be a relatively straightforward reform, bringing Australian law into line with at least two other major jurisdictions – most notably, California's *Training Data Transparency Act*, as well as the European Union. By modelling an Australian TDT requirement on one or both of these very similar laws, Australian law could be interoperable with those other major AI economies, while having the flexibility to meet Australia-specific priorities.

California's *Training Data Transparency Act* took effect this year. It requires a developer of a generative AI system or service, made available in California, to publish a "high-level summary of the datasets used in the development of the generative artificial intelligence system or service", including the dataset sources, ownership, format, volume, collection periods, copyright status, personal data, and synthetic data.⁹ While x.AI is mounting a constitutional challenge to the Californian law, OpenAI, Anthropic and Google/Alphabet have decided not to join this court challenge, and instead to work within California's data transparency regime. Leading companies – including Google, Meta, Microsoft and OpenAI, alongside Swiss AI, SpeakLeash, Hugging Face and Bria – have already issued public disclosure statements under California's and/or the EU's respective TDT laws.¹⁰

Recommendation

The Australian Government should include a training-data transparency requirement in the Australian Standards for AI, which are currently being developed. In developing this requirement, the Government should provide an

opportunity for public input via its upcoming public consultation process on the Standards.

Targeted reform to address tech-enabled worker surveillance

Overview

AI and related technologies are creating new ways to monitor workers. Thoughtful monitoring can support well-run, safe workplaces. However, in the age of AI, technology is combining with increased flexible and remote working arrangements to create a rising tide of harmful worker surveillance.

This problem is not addressed by existing laws, which are complex and confusing for employers and workers alike. Current law also fails to provide adequate protections for workers subject to surveillance. Law reform is necessary and urgent.

In this submission HTI recommends the Australian Government adopt a practical law reform solution, which is set out in more detail in HTI's forthcoming report, *Drawing the Line: Tech-enabled Surveillance of Australian Workers* (October 2026). HTI's reform proposals would:

- introduce a requirement in the Fair Work Act that any worker monitoring be 'fair and reasonable' outlining flexible factors that apply
- set up a dedicated complaints stream in the Fair Work Commission to hear privacy-related worker complaints
- amend the Fair Work Act to ensure that enterprise bargaining agreements and Modern Awards can build on the protections in the proposed 'fair and reasonable' requirements.

The Australian Government must lead the law reform response, by amending employment law to distinguish reasonable monitoring from harmful surveillance.

HTI's recommendations are the culmination of a 10-month project focused on designing a practical and implementable law reform solution. HTI's March 2026 Snapshot Report, [Surveillance Creep](#), described the rise of tech-enabled worker surveillance, and set out our preliminary views regarding reform.¹¹ In the months since, HTI has tested and refined this proposed reform through deep consultation with unions, industry groups, legal experts and government stakeholders.

Rise in tech-enabled worker surveillance

Worker monitoring is rapidly increasing in Australia. Monitoring tools range from bespoke surveillance tech, like cameras enables with facial recognition technology (FRT), to products with embedded surveillance capabilities – including software as common as Microsoft Teams. These tools are being rolled out across the full range of Australian workplaces.¹² Office workers, delivery drivers, factory technicians and shop assistants are all experiencing this increased surveillance.

While workers increasingly report harm from unreasonable surveillance, most workers simply don't know the true extent of surveillance they are subjected to.¹³ This awareness gap is quickly closing. There is growing concern, especially from Australian workers and unions, about unchecked surveillance.¹⁴

Examples of tech-enabled surveillance causing harms to workers

Woolworths' 'framework' was a factor contributing to the 2024 Woolworths strike.¹⁵ The framework relied on AI to push workers to meet productivity metrics. These

kinds of productivity tools can have the effect of pressuring workers to work harder and faster, for no additional reward, under the threat of punitive repercussions. This can threaten their health and safety.

The Victorian company **Safetrac** used work-issued laptops to record audio of staff working from home for up to eight hours a day, without their knowledge or consent.¹⁶ The software was capable of capturing private conversations within families, and confidential information discussed with clients.¹⁷ This highlights the level of intrusion of some employers into the home and family lives of remote workers.

A recent US lawsuit alleges that **Meta** used data from performance rankings, and keystroke and activity-monitoring data, to target workers for mass layoffs. The performance rankings and productivity metrics, allegedly relied on by the AI tools, were not recorded when workers were on medical or family leave. The claimants allege that, as a result, employees who took pregnancy, medical, or other forms of approved leave received a lower rating – in some cases resulting in discrimination.¹⁸

Clear need for reform to address tech-enabled worker surveillance

Australian law should draw a clear line between justified worker monitoring and unreasonable or harmful surveillance. However, our law is complicated, confusing and riddled with gaps.

At the federal level, workplace laws do not directly regulate worker surveillance, and the Privacy Act includes an ‘employee records exemption’ which means that the Act does not regulate an employer’s handling of personal data relating to the employment of its employees.¹⁹ This creates a gap between these two frameworks, which is inadequately addressed by incomplete and inconsistent state and territory laws. Meanwhile, state and territory surveillance laws do not offer clear rules. They are inconsistent with each other on fundamental issues such as requirements for consent; and do not adequately take into account new technologies such as AI.²⁰

In practice, employers assume they are legally permitted to engage in a form of worker monitoring or surveillance if the worker has given their consent (for example, in their employment contract), but such consent is rarely genuine, free and informed. Workers rarely have the information they need to understand precisely how they will be monitored, and even when a worker has this information, refusing to be monitored is likely to jeopardise their employment.

HTI’s consultation process revealed broad agreement among stakeholders representing workers and employers that our current law is failing. Workers lack crucial protections from surveillance-related harms. At the same time, employers are unclear on when and how they can monitor their workers. There is a strong impetus for reform on both sides.

HTI’s reform recommendations: Worker monitoring should be fair and reasonable

HTI’s reform proposals are designed to be practical and readily implementable. They are relatively straightforward to introduce, and would provide crucial protections by addressing key harms and gaps.

Substantive protections for workers

Currently, surveillance of workers is primarily justified through the provision of consent, often through vague monitoring clauses in employment contracts – which rarely constitutes genuine, free and informed consent.

As discussed below (p 14) the Australian Government has already committed to introducing a general requirement that all personal information, covered by the Privacy Act, must be handled 'fairly and reasonably'. These requirements have now been outlined in the exposure draft of the Privacy Amendment (Personal Data Protection) Bill 2026.²¹ However, due to the employee records exemption in the Privacy Act, the introduction of the fair and reasonable test would not apply to the employment context.

HTI's approach would adapt the Albanese Government's proposed 'fair and reasonable' factors, and apply them to the specific worker monitoring context – by introducing them in the Fair Work Act. HTI has tested and outlined how the fair and reasonable factors may be practically adapted for the workplace - see **Appendix A** for some examples. In practice, the reform would draw a clear line between reasonable monitoring of workers, and unreasonable surveillance.

When the 'employee records' exemption was introduced into the Privacy Act in 2000, the stated rationale was that 'the handling of employee records is a matter better dealt with under workplace relations legislation'.²² However, the Fair Work Act has never been expanded to regulate how employers collect and use information about workers. HTI's proposed reform would address this longstanding gap, while maintaining a consistent approach between Australian privacy and workplace laws.

Accessible complaints mechanism

In introducing this reform, the Fair Work Commission should provide for a dedicated complaints stream for privacy-related workplace complaints, to provide an accessible avenue for worker surveillance issues to be heard and mediated. This was previously recommended by the House of Representatives Standing Committee on Employment, Education and Training in its *Future of Work Report*.²³

A dedicated privacy complaints stream in the Fair Work Commission would help ensure that privacy issues are considered in the context of other workplace claims, noting that surveillance data may be used as a basis for taking adverse action against workers, dismissing them, or otherwise impacting their workplace rights. This would prevent privacy issues being de-prioritised in complaints processes, and would build the Fair Work Commission's expertise on the intersections between privacy and workplace matters.

Support for collective bargaining

If the proposed 'fair and reasonable' requirement were included in the Fair Work Act, it would be logical to also include a provision that applies to consultation on worker surveillance in enterprise bargaining agreements (EBAs) and modern awards. A model consultation clause for EBAs and awards could provide for consultation where an employer proposes to introduce new surveillance tools or methods.

The model consultation clause would serve as the default, with unions and employers also having the opportunity to negotiate tailored worker surveillance clauses articulating what is fair and reasonable in particular industries and workplaces. Negotiated worker surveillance clauses would be restricted from undermining the minimum protections outlined in the fair and reasonable test. As such, unions would have a strong initial footing upon which to commence negotiations, and those workers that do not have the backing of a union would still be covered by the baseline protections in the Fair Work Act.

Clear and practical guidance

Guidance issued by regulators such as the Fair Work Ombudsman would assist employers to understand and comply with new and existing laws. Regulators can provide authoritative or supportive guidance on legal compliance when the guidance is

directly tied to existing primary legislation – as such, the introduction of new substantive protections would provide an important hook for regulators to provide certainty about employers' responsibilities in this context.

Reform must be led by the Federal Government

The Australian Government has a clear mandate to undertake these reforms, having put workers at the centre of the National AI Plan. In July 2026, Prime Minister Albanese emphasised the Government's work on navigating 'AI's role in the workplace'.²⁴ AI safety in the workplace is also one of the Government's five AI consumer safety priorities.

The Government has recognised that this is not a distant problem. On the contrary, workers are experiencing the harms of unchecked worker surveillance right now, and the Australian community expects the government to act to protect them.

National reform must be led at the federal level to address the growing reality of regulatory fragmentation. The New South Wales and Victorian Governments have recognised the urgency of the problem and have independently initiated reform processes.²⁵ Federal leadership can ensure that Australians workers have access to consistent protections regardless of their location, and to prevent compounding regulatory complexity. The reform process should harmonise Australian law and reduce areas of regulatory overlap – which will require coordination with states and territories.

Protecting workers from the harms of surveillance is not only about ensuring the safety of individual workers. It is about restoring trust, fairness and dignity to the way we work. If we get these basics right, Australia can weather the storm of technological change and uphold our core values.

Recommendation

The Australian Government should lead national worker surveillance reform by:

- a) **introducing a requirement in the Fair Work Act that any worker monitoring be 'fair and reasonable' outlining the relevant factors that apply to this context**
- b) **establishing a dedicated complaints stream in the Fair Work Commission to hear privacy-related worker complaints**
- c) **amending the Fair Work Act to ensure that enterprise bargaining agreements and Modern Awards can build on the protections in the proposed 'fair and reasonable' requirement**
- d) **supporting regulators such as the Fair Work Ombudsman to issue practical guidance on how to apply new and existing laws in the worker surveillance context.**

Law to govern automated decision making

The urgent need for an automated decision-making law

Automated decision making (ADM) has the potential to increase the efficiency of high-volume, non-discretionary decisions. However, as government continues to adopt ADM systems, appropriate safeguards are required to ensure these systems are effective, and operate lawfully and accountably. Crucial safeguards are outlined in HTI's submission to the Attorney-General Department's (AGD) *Consultation on the Use of Automated Decision Making in Government*.²⁶

The Albanese Government first committed to legislating an automated decision-making framework (ADM legal framework) in 2023, thereby implementing a key recommendation of the Robodebt Royal Commission. In the absence of an ADM legal framework, the Government has increased its use of automation especially in service delivery.

While many instances of ADM are low risk, HTI hold grave concern about a number of the Government's ADM initiatives, implemented since 2023 without appropriate safeguards. As outlined in HTI's submission to Senate Community Affairs Legislation Committee's inquiry, the automation provisions in the recently-passed *National Disability Insurance Scheme Amendment (Securing the NDIS for Future Generations) Act 2026* explicitly authorise ADM to an extent that is, to our knowledge, unprecedented in Australian law.²⁷

This is not merely a hypothetical risk. Real harm is being experienced now – by large numbers of vulnerable Australians – as a result of poorly designed and regulated ADM. Well-known examples include:

- **the integrated assessment tool (IAT)**, introduced by the Department of Health, Disability and Ageing in July 2024. The IAT is used to assess funding packages for older Australians accessing aged care services. Human assessors are required to accept the system generated outcomes that the IAT provides.²⁸ As of March 2026, there had been 834 review requests,²⁹ accompanied by a 50% surge in demand for advocacy services since its introduction.³⁰ The IAT is currently being investigated by the Commonwealth Ombudsman.³¹
- **the Targeted Compliance Framework**, administered by the Department of Employment and Workplace Relations (DEWR), has been plagued with problems associated with inaccurate suspension and cancellation of jobseeker payments through automation. In 2025, the Commonwealth Ombudsman found that DEWR's cancellation of income support was not lawful.³² The Framework has been flagged as an 'unquantifiable liability' in this year's budget.³³
- **automated historical debt letters** from the Australian Tax Office (ATO). In 2024, the ATO sent up to 200,000 boilerplate, automated letters to Australian taxpayers and tax agents, stating that they had 'on-hold' historical tax debts. The letters did not provide detail about how or why the debts had arisen, and caused confusion and distress to recipients. The ATO publicly apologised.³⁴

Key safeguards required in an automated decision-making framework

A number of leading non-government organisations, led by ACOSS and HTI, recently wrote to the Attorney-General outlining some of the key safeguards necessary in an ADM legal framework. They are:

- **Parliament should determine which types of decision may be automated.** The determination whether to allow automation for a category of government decision making (such as the availability of services under the National Disability Insurance Scheme) should be made by Parliament, given that this enables effective democratic oversight. This responsibility should not be delegated to a Minister or an unelected official.
- **Generally, decisions involving discretion or the exercise of evaluative judgment should not be automated.** The ADM legal framework should make clear that the default position is that ADM should not be used for any discretionary element of the decision-making process, nor should it be used where there is a

likelihood that it will narrow the exercise of discretion. While there may be exceptional circumstances, which could justify automating discretion (for example, by enabling favourable discretionary decisions to be made via ADM), this requires specific justification and greater oversight. This principle is well-understood: several Government authorities including the Commonwealth Ombudsman and the Australian Human Rights Commission have cautioned against automating discretionary decisions.³⁵

- **People should be able to seek review of automated decisions.** The law should enable a person who wishes to challenge an automated decision to do so using accessible and appropriate review processes. The use of ADM should not have the effect of denying or reducing review rights for people affected by government decisions. If a decision would be reviewable if made by a human, it should also be reviewable if made through automation. This should include:
 - internal review by a more senior official, which is the most common, cost-effective and accessible pathway to address inaccurate or unfair decisions³⁶
 - extend to external merits review (by a tribunal)
 - judicial review.
- **Anyone affected by an automated decision should be given reasons for the decision.** When a decision is made affecting a person's legal or human rights, or otherwise significantly impacting them, they should be provided with a plain language explanation of the legal and factual basis for the decision.
- **The Government should give proactive consideration to human rights, including impacts on vulnerable and marginalised communities.** Before adopting ADM, government should be required to proactively assess the human rights of those likely to be affected, including giving particular consideration to groups experiencing vulnerability or marginalisation. ADM systems that have an unjustified impact on human rights should not be implemented.

Recommendation

The Australian Government should fulfill its commitment to implement recommendation 17 of the Robodebt Royal Commission by introducing a Bill to regulate automated decision making in government. The Bill should contain the necessary safeguards to ensure that ADM operates effectively, lawfully and accountably by requiring:

- **Parliament, not a minister or unelected official, to determine when it is appropriate to automate a category of government decision making**
- **that decisions involving discretion or evaluative judgment generally should not be automated**
- **anyone affected by an automated decision should be given reasons for the decision, and be able to seek effective review of that decision**
- **proactive consideration of the human rights of people likely to be affected by automating a category of decision making before this is permitted.**

Modernising Australian privacy law

HTI welcomes the exposure draft of the Privacy Amendment (Personal Data Protection) Bill 2026 (the exposure draft). If implemented, the exposure draft would modernise and strengthen the *Privacy Act 1988* (Cth) (Privacy Act).

HTI will provide a detailed submission in response to the Attorney-General's Department consultation process, especially to better protect Australians against misuse of their personal data in the context of new technologies like AI. In summary, HTI proposes two categories of privacy reform. First, HTI recommends that the exposure draft should be amended:

- to improve the drafting of some key provisions, with a view to better achieving the Government's stated intent, taking into account its existing reform commitments made in the whole-of-government response to the Attorney-General's Privacy Act Review Report (the AGD report).³⁷ HTI's proposed drafting improvements are summarised in a table, which is set out in the Appendix to this submission
- to include a small number of substantive changes to the exposure draft to address high-priority issues that would not otherwise be captured by the proposed reforms - including with respect to high-risk biometric and other surveillance technologies such as smart glasses and facial recognition technology.

Second, HTI urges the Committee to recommend a small number of privacy-related reforms that appear to be outside the scope of the current reform process – for example, the removal of the small business exemption.

The Australian Government should implement committed reforms outlined in the exposure draft

HTI welcomes key reforms in the exposure draft that would introduce important commitments made by the Australian Government in response to the AGD report. Of particular significance are the inclusion of the 'fair and reasonable' test, and expanded definitions, including of 'personal information', which would bring the Privacy Act into the modern era.

While the exposure draft introduces a range of reforms directly recommended by the AGD report, there are some additional reforms that have been included in the form of exceptions, qualifiers and scope limitations, as well as drafting changes that substantively alter existing commitments. These additions and drafting changes also introduce some new ambiguities regarding how the Privacy Act is to be interpreted and applied. HTI recommends that certain provisions be amended to ensure that they do not inadvertently weaken existing and new proposed protections in the Act. These are outlined in the table in Appendix B.

Recommendation:

The exposure draft of the Privacy Amendment (Personal Data Protection) Bill 2026 should be passed with HTI's proposed amendments (see Appendix B) to ensure that the reform makes good on the Australian Government's prior commitments to privacy law reform.

Amendments to the exposure draft to address high-priority issues

There remain outstanding gaps in the Privacy Act that must be addressed so that Australians are adequately protected, and privacy rights appropriately enforced. HTI recommends that two priority reforms be included in the exposure draft – each would

substantively address serious harms affecting Australians, and would require simple and straightforward amendments to the existing exposure draft.

Protections for biometric surveillance

Targeted reforms are needed to address biometric and other tech-enabled surveillance, such as smart glasses and other wearable devices. Such products and services often use AI, such as FRT, which is not regulated directly, and brings significant human rights risks.

We have seen a rapid expansion of FRT used in Australia across the public and private sectors. Live FRT is currently being trialled by the Western Australia Police Force, has been adopted by major retailers such as Bunnings and Kmart, and is increasingly being used at sporting clubs and stadiums.³⁸ Increasingly popular smart glasses also have recently sparked intense public concern, and are capable of being used for many harmful and criminal purposes, including and harassment.³⁹ Many smart glasses products also in-built FRT capability.⁴⁰ The unchecked diffusion of these technologies raises the real risk of mass surveillance.

The exposure draft does not directly address the implications of these technologies and the existing provisions are not adequate to address the risks – a dedicated response is required. HTI has previously outlined a model law for FRT in *Facial recognition technology: Towards a model law*.⁴¹

In the short term, HTI recommends that the exposure draft be amended to empower the Privacy Commissioner to develop a code under the Privacy Act for biometric and surveillance technologies, with a view to addressing the risks associated with smart glasses and other similar products and services. In the medium term, HTI recommends that the Government implement the recommendations from this report, which would introduce necessary safeguards, and set an appropriate balance that addresses the risks of harm associated with FRT, while encouraging positive innovation with FRT.

Direct right of action

Where a company or government agency, covered by the Privacy Act, breaches the Australian Privacy Principles, it can be difficult and very slow for an individual to enforce their rights via a relatively small regulator, which has very limited resources. As a result, HTI recommends the Act be amended to provide a direct right of action, to better enable individuals to seek remedies in the courts for privacy breaches that cause harm. Allowing individuals to apply directly to the courts for relief when their privacy is interfered would improve the pathways available to uphold privacy rights under the Act.

Recommendation

The Australian Government should amend the Privacy Amendment (Personal Data Protection) Bill 2026 to include:

- a requirement that the Privacy Commissioner develop a code on biometric and other surveillance technologies, modelled on s 26GC in the current Privacy Act
- a direct right of action where a regulated entity breaches the Australian Privacy Principles.

Additional privacy law reforms

This Committee should recommend that the Government make good on its other committed privacy law reforms. In particular, the Privacy Act includes several exemptions that leave Australians unprotected in everyday contexts. These include:

- the employee records exemption, which excludes the Privacy Act from regulating an employer's handling of personal data relating to the employment of its employees.⁴² This exemption, combined with gaps in employment laws, mean that Australian workers are largely unprotected from harms related to worker surveillance. HTI's proposal to reform the Fair Work Act discussed above (p 11) would address this issue through employment law reform, rather than via reform to the Privacy Act.
- the small business exemption which excludes approximately 94% of businesses in Australia from compliance with the Privacy Act.⁴³ This anomalous exemption leaves consumers exposed and unprotected, and should be repealed.

Recommendation

The Australian Government should implement outstanding Privacy Act reform commitments prior to the next Federal election.

The OAIC must be sufficiently resourced to enforce the Privacy Act

New laws only protect people if they are adequately enforced. The Office of the Australian Information Commissioner (OAIC) is facing increasing demand: to illustrate, it received 11,800 matters in the 2025–26 financial year, compared to 7,717 received in 2024–25.⁴⁴ Despite this, the OAIC was allocated \$36.6 million in the 2026-27 Federal Budget – down from \$39.8 million in 2025-26, and representing an 8 per cent cut to the agency's departmental appropriation.⁴⁵ The implementation of the Exposure Draft would serve to compound existing demand on the OAIC. In our data-driven world, Australians routinely experience privacy and AI related harms, and the OAIC must be in a position to respond appropriately. At the same time, businesses require guidance on how to comply with new provisions, which the OAIC is best placed to provide. New reforms should be packaged with increased funding for the OAIC so that they can continue to fulfil their remit.

Recommendation

The Australian Government should make provision to resource the OAIC adequately to ensure that new and existing privacy protections are appropriately understood and enforced.

Appendix A

Worker surveillance: Fair and reasonable requirement factors

Factor	Example
Is this use of data <i>reasonably necessary</i> for the functions/activities of the organisation?	It would not be reasonably necessary to use location tracking apps for the purpose of monitoring in-office attendance
Would an affected individual <i>reasonably expect</i> this use of their personal information?	Workers would not reasonably expect to be monitored outside of work hours
Is there transparency about the means and the purposes for the use of information?	A high-level monitoring policy that does not explain the kinds of tools in use, and the purposes they are used for, would not be sufficiently transparent
What is the risk of <i>harm</i> , and is the impact <i>proportionate</i> to the benefit?	Use of a productivity tool that is likely to discriminate against workers with disability would risk unjustifiable harm Safeguards such as routine audits and transparency measures may reduce the likelihood and severity of harms relative to the benefits

Appendix B

Table 1: Proposed amendments

Reform element	Exposure Draft Bill	HTI's view	Important amendments needed for the Exposure Draft Bill
New fair & reasonable test	Proposed new APP 3	HTI supports the inclusion of a new provision that requires APP entities to handle personal information fairly and reasonably. This reform could: • combat the over-reliance by APP entities on consent to avoid their privacy obligations, especially where such consent is often not genuine • ensure that APP entities give greater weight to the privacy rights of individuals before handling their personal information.	In addition to more minor wording changes, there are three main problems with the drafting of this provision in the Exposure Draft. First, proposed new APP 3.2(b) states that, in determining whether it would be fair and reasonable to collect, use or disclose personal information, an APP entity must consider “whether the collection, use or disclosure of the information <i>relates to</i> one or more of the APP entity’s functions or activities”. This differs from the Government’s original proposed wording which was “whether the collection, use or disclosure is <i>reasonably necessary</i> for the functions and activities of the organisation or is reasonably necessary or <i>directly related</i> for the functions and activities of the agency” (emphasis added). This factor addresses whether an APP entity has a legitimate purpose for handling the personal information in the first place. APP entities should have a good reason for handling an individual’s personal information – hence the original wording asks whether this is <i>reasonably necessary</i> for an organisation’s functions or activities (and a similar standard for government agencies). If an APP entity could satisfy this factor merely because the personal information handling <i>relates to</i> its functions/activities, it would allow significantly more personal data collection and use. For example, the Exposure Draft wording would allow a real estate agent to gather personal data from renters, to determine whether they could afford to pay higher rental fees, because this would be related to the service the agent is providing. But this wouldn’t satisfy the factor under the original wording, because such information isn’t <i>reasonably necessary</i> to provide the rental service. The new wording would therefore be a step backwards.

			Second, proposed new APP 3.2(e) asks whether the individual is ‘provided with genuine choice’ in relation to the collection, use or disclosure of information. HTI recommends that proposed APP 3.2(e) be redrafted to require consideration of whether the individual has given consent. Merely giving the opportunity for genuine choice, without assessing whether someone has taken that opportunity, would re-introduce one of the problems with sham consent, which this Bill is trying to address. In any case, the fair and reasonable test was designed to apply in <i>addition</i> to consent requirements. The Exposure Draft Bill includes a new definition for consent, which HTI welcomes. This definition would help improve consent processes, which are necessary but not sufficient on their own. Thirdly, the proposed fair and reasonable test excludes one original factor from the AGD Report – a requirement for entities to consider ‘the kind, sensitivity and amount of information being collected, used or disclosed’. The amount and nature of personal data being handled are directly relevant to whether the APP entity is acting fairly and reasonably. For example, collecting more personal data increases the risk to the person’s privacy, and this should be justified. Hence, this consideration should be included either as a standalone fair and reasonable factor as originally intended, or as an explicit element of the proportionality factor (proposed APP 3.2(f)). Finally, HTI notes that the proposed fair and reasonable requirements are currently articulated as non-essential indicia to be considered holistically – entities would not have to satisfy every legislated factor to meet their obligations. HTI recommends that some of the fair and reasonable factors be classified as essential indicia. This would ensure that entities take steps to comply with baseline considerations when handling personal information. HTI recommends that proposed APP 3.2(b) (redrafted as above), APP 3.2(e) (redrafted as above) and APP 3.2(f) be treated as essential requirements.
--	--	--	---

Purpose limitation	Repeal current APP 6	The repeal of current APP 6 would remove the core purpose-limitation requirements, which is not captured by the new fair and reasonable test. Current APP 6 should be retained, so that the new reforms do not inadvertently reduce existing protections.	Under current APP 6, APP entities cannot use or disclose personal information for a secondary purpose, unless consent has been given or specified condition are met. The repeal of APP 6 would remove this requirement – and it is not otherwise captured by the fair and reasonable test provisions. Purpose limitation is a vital privacy protection, because it sets a default restriction on how personal information can be handled, based on an APP entity's most relevant justification – its 'primary purpose'. Handling personal information for a secondary purpose should require more specific justification – as the Privacy Act currently provides. Removing this protection would weaken the Privacy Act. Therefore, current APP 6 should be retained.
Exceptions for requirements to obtain consent for sensitive information	Proposed APP 4.3 and 4.4	The new exceptions to requirements to obtain consent for the collection of sensitive information should be removed, or at least more narrowly scoped.	The Exposure Draft proposes two new exceptions to consent requirements for the collection of sensitive information. These exceptions were not recommended in the AGD Report. Proposed APP 4.3 would create an exception where personal information is collected from a publicly-available document. This includes such documents that are available subject to a 'barrier to access', such as a fee or account registration, provided the barrier could be overcome by an ordinary member of the public. This exception could apply to, for example, sensitive information obtained from: a data broker upon payment of a fee; criminal records databases; private social media pages or forums for people with protected attributes – such as support groups for people with mental health conditions. If this exception is to be retained, the definition of publicly available documents should be amended to <i>exclude</i> information where there is a 'barrier to access'. Proposed APP 4.3 would provide that consent is not required where collection is strictly necessary to provide or deliver a good or service explicitly requested by an individual, and where the good or service cannot be provided in a less privacy intrusive manner. In HTI's view, it is no less important for individuals to know and consent to the use of their sensitive information, regardless of whether they've requested the relevant good/service or not. This exception should therefore be removed.

			HTI also notes that if these exceptions were introduced, they would be inconsistent with higher standards for sensitive information contained in ss 45, 46 and 48 of the <i>Digital ID Act 2024</i> (Cth), which were intended to align with future Privacy Act reforms as recommended by the AGD Report.
Permitted general situations	Item 17 (replacement of s 16A)	Proposed APP 3.3(b) should be amended to delete the word 'collection'. This would have the effect of bringing current protections across, that would otherwise be lost through the repeal of APP 3. Additionally, proposed wording changes to PGS2 should be clarified via a legislative note, to assist with interpretation of the new terminology.	In a permitted general situation (PGS), the Privacy Act requirement to obtain consent for sensitive information does not apply. A PGS can be relied on to introduce high-risk technologies, such as facial recognition in retail and policing contexts. Changes to PGS provisions were not recommended by the AGD Report. Proposed APP 3.3(b) provides that the new fair and reasonable requirement would not apply to PGSs. The Exposure Draft would also repeal APP 3.5, which would remove the requirement that collection of personal information be 'lawful and fair' – even in a PGS. If current APP 3.5 is removed, then proposed APP 3.3(b) should be amended to delete the word 'collection'. This would have the effect of bringing the current protection across. Additionally, the Exposure Draft would amend PGS 2 to replace 'misconduct of a serious nature' with 'wrongdoing of a serious nature'. The Consultation Paper explains that this is intended to be 'broader than misconduct', and include conduct by a person acting in a private capacity – such as in cases where an entity suspects a customer may be experiencing financial abuse. HTI recommends that the Bill define 'wrongdoing' as behaviour that amounts to serious misconduct, and it should also include a statutory note to make clear that wrongdoing in this context would include where an entity suspects a person is exploiting a customer's vulnerability, or misusing enduring power of attorney for personal gain. Finally, HTI recommends that in the PGS table, Item 1 column 3 should delete the words 'for sensitive information' so that the exception is not widened beyond its current articulation in the Privacy Act.

Notice	Proposed APP 5.1, 5.3	HTI supports clarification regarding the form of notices informing of the collection of personal information. This should be supplemented by <i>existing</i> requirements in current APP 5 for the content of notices, rather than the more limited approach in proposed APP 5.1.	New requirements for the form of collection notices directly implement AGD Report recommendations. However, the AGD Report proposed this reform to be introduced alongside the <i>existing</i> list of matters to be included in notices, outlined in APP 5.2. These matters would be substantively reduced by proposed APP 5.1. Thorough notices are important to assist individuals understand how their data is being used, and enforce their rights. HTI recommends that notice content requirements in APP 5.2 be retained.
Direct marketing	Proposed APP 7	HTI welcomes new requirements for digital marketing, including for opt outs, which would apply in addition to the fair and reasonable test. However, these provisions are significantly undermined by a broad exception for ‘ad-supported services’ – which should be removed.	The Exposure Draft defines ‘ad-supported services’ as entities for whom the ‘marketing communications to individuals who use the service is itself a source of revenue for the organisation’. If individuals opt-out of these services, the Exposure Draft would enable them to offer the service “<i>on terms that differ from the terms on which the service or element is offered to individuals who receive direct marketing, as long as the different terms provide the individual with genuine choice to continue.</i>” The direct marketing provisions apply to targeted advertising that uses personal information – including in ways that are manipulative, opaque and exploitative. They do not capture advertising that does not rely on personal information. There should naturally be a high bar for advertising that relies on personal information, especially given the risk of harm is high. The proposed exception for ad-supported services would permit a wide array of organisations and platforms, including social media services, to offer a <i>worse</i> service for people who opt-out of direct marketing using their personal information – this would not create conditions for people to provide genuine consent, and could indirectly enable the kinds of manipulative practices that these new protections are intended to prevent. This exception was not recommended by the AGD Report – in fact, the AGD Report recommended ‘unqualified rights’ to opt out of direct

			marketing. There may be cases where it is reasonable for ad-supported services to offer an alternative experience for those who opt out of direct marketing – for example, customers that do not opt out of direct marketing on a shopping site may receive personalised recommendations or feeds; customers who opt out would not have access to this feature. However, the Exposure Draft Bill contains a wider exception than this. Its breath would undermine the protective intent of the provisions. If the exception cannot be appropriately narrowed, it should be removed. As with the sensitive information exception above, these provisions would be inconsistent with privacy protections in the Digital ID Act which generally prohibit the use or disclosure of personal information for marketing purposes, subject to very limited exceptions.⁴⁶
Right to erasure	Proposed schedule 4, part 2.	HTI supports a right to erasure. The current drafting would allow the right to be exercised only against 'large digital platforms'. This should be redrafted as a general right to erasure.	The AGD Report proposed a general right to erasure, allowing individuals to have their personal information erased, which would also address third parties who hold data. That approach mirrors laws in jurisdictions such as the EU and UK. The Exposure Draft would allow this right to be exercised only as against 'large digital platforms' (with gross annual revenue of \$500 million or more, or with 2.5 million or more average monthly end users). There is no clear practical or principled justification for this restriction to the right to erasure. The qualification that the right only applies to 'large digital platforms' should be deleted.
OAIC powers	TBD	HTI supports proposals for new powers and processes that would enable the OAIC to more effectively enforce the Privacy Act. HTI recommends that the OAIC be granted the power to issue substantiation notices as part of this package.	Substantiation notices are an important power for regulators in the digital age. When substantiation notices are issued, a person must produce information or documents capable of substantiating representations made by that person. This power would be especially useful in respect of products and services that rely on AI, because it can be very difficult for regulators to determine how such products and services use personal information. Providing the OAIC with this power would align it with other Australian regulators. In 2009, the ACCC and ASIC were both conferred the power to issue substantiation notices to protect consumers because 'the lack of an ability to quickly and easily

			require information to substantiate claims made in representations by businesses' was a 'key gap in the powers of the ACCC and ASIC'. ⁴⁷
--	--	--	---

Table 2: Other welcome reforms

Reform element	Exposure Draft Bill	HTI's view
Definitions of personal and sensitive information	Proposed ss 6FD, 6FE and 6FF	HTI welcomes these updated definitions which would broaden the scope of the Privacy Act regime to encompass the ways in which data can be used to identify, profile and target individuals in the digital world.
Definition of consent	Proposed 6AAB	HTI welcomes the updated definition of consent, which would serve to improve the quality of consent obtained from individuals, in line with AGD Report recommendations.
Strengthened requirements for data deletion, data security and data breach notification	Proposed schedule 3	HTI welcomes a range of proposed provisions that would introduce new requirements for entities to take steps to protect personal data; proactively consider whether to destroy data that is no longer needed; and take reasonable steps to either destroy or de-identify unneeded information, as well as strengthened obligations on entities to respond to and contain data breaches. This will assist in preventing and responding to misuse and interference with data and poor data handling practices that cause harm to individuals.
Requirements for trading of personal information	Proposed APP 4.2	HTI welcomes the inclusion of provisions relating to the trading of personal information, which would cover a broad range of arrangements in which personal information is disclosed as part of an exchange, with related consent requirements. This implements an AGD Report recommendation.

Endnotes

- ¹ Nicole Gillespie et al, *Trust, Attitudes and Use of Artificial Intelligence: A Global Study 2025* (Report, The University of Melbourne and KPMG, 2025) 45.
- ² Minister Anika Wells, Minister Amanda Rishworth, Attorney-General Michelle Rowland, Minister Tim Ayres, Assistant Minister Andrew Lee, Assistant Minister Andrew Charlton, 'AI Consumer Safety Priorities' (Joint Media Release, 20 July 2026) <<https://ministers.ag.gov.au/media-centre/ai-consumer-safety-priorities-20-07-2026>>.
- ³ Joint Select Committee on Artificial Intelligence, Parliament of Australia, *Terms of Reference* (August 2026) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Artificial_Intelligence>.
- ⁴ Minderoo Foundation and Talbot Mills polling (March 2026), published in Human Technology Institute, *Surveillance Creep: technology-enabled worker surveillance* (March 2026) 8 <<https://www.uts.edu.au/news/2026/03/australian-law-must-protect-workers-from-harmful-tech-enabled-surveillance/contentassets/hti-snapshot-report-worker-surveillance.pdf>>.
- ⁵ Herbert Smith Freehills Kramer 'The Future of Work Report 2021', *Insights* (Web Page) <<https://insights.hsfkramer.com/fow2/p/9>>.
- ⁶ Zoe Jay Hawkins and Johanna Weaver, *Earning Trust: Unlocking AI Adoption for Australians* (Policy Spotlight, Tech Policy Design Institute, May 2026) <<https://techpolicy.au/earning-trust/>>.
- ⁷ 'GPAI Training Transparency' *AI Accountability Lab* (Web Page) <<https://aial.ie/research/gpai-training-transparency/>>.
- ⁸ Artem Serov, 'EU AI Act & Copyright: A Practical Guide for Developers', *Hugging Face* (Web Page) <<https://huggingface.co/blog/ArtemSerov/ai-copyright-compliance>>.
- ⁹ *Generative AI Training Data Transparency Act 2024* (AB 2013) (California). For a brief explainer of this law see, eg, Gary Kibel, 'AI legal updates: California's AI Training Data Transparency Law Takes Effect' *David Gilbert Law* (Webpage) 23 January 2026 <<https://www.dglaw.com/ai-legal-updates-californias-ai-training-data-transparency-law-takes-effect/>>.
- ¹⁰ Dick Blankvoort, Harshvardhan Pandit, Maximilian Gahntz, 'Quality Assessment of Public Summary of Training Content for GPAI models required by AI Act Article 53(1)(d)' (9th ACM Conference on Fairness, Accountability, and Transparency, Montreal, Canada, June 25-28 2026) (preprint).
- ¹¹ Human Technology Institute, *Surveillance Creep: Tech-enabled Surveillance of Australian workers* (March 2026) <<https://www.uts.edu.au/news/2026/03/australian-law-must-protect-workers-from-harmful-tech-enabled-surveillance/contentassets/hti-snapshot-report-worker-surveillance.pdf>>.
- ¹² Human Technology Institute, *Surveillance Creep: Tech-enabled Surveillance of Australian workers* (March 2026), 10 <<https://www.uts.edu.au/news/2026/03/australian-law-must-protect-workers-from-harmful-tech-enabled-surveillance/contentassets/hti-snapshot-report-worker-surveillance.pdf>>.
- ¹³ Human Technology Institute, *Surveillance Creep: Tech-enabled Surveillance of Australian workers* (March 2026), 8 <<https://www.uts.edu.au/news/2026/03/australian-law-must-protect-workers-from-harmful-tech-enabled-surveillance/contentassets/hti-snapshot-report-worker-surveillance.pdf>>.
- ¹⁴ See, e.g. Unions NSW, 'Surging Worker Anxiety about Artificial Intelligence' (Media Release, 5 February 2026) <<https://unionsnsw.org.au/media-release/surging-worker-anxiety-about-artificial-intelligence>>; Zoe Jay Hawkins and Johanna Weaver, *Earning Trust: Unlocking AI Adoption for Australians* (Policy Spotlight Report, May 2026) 1 <<https://techpolicy.au/earning-trust/>>.
- ¹⁵ Ariel Bogle, "'Stop All Time Wasting': Woolworths Workers Tracked and Timed under New Efficiency Crackdown", *The Guardian* (online, 23 October 2024) <<https://www.theguardian.com/business/2024/oct/23/woolworths-staff-efficiency-productivity-crackdown-timed>>.

-
- ¹⁶ David Marin-Guzman, 'Company Turned Laptops into Covert Recording Devices to Monitor WFH', *Australian Financial Review* (online, 24 August 2025) <<https://www.afr.com/work-and-careers/workplace/company-turned-laptops-into-covert-recording-devices-to-monitor-wfh-20250822-p5mp0z>>.
- ¹⁷ David Marin-Guzman, 'Company Turned Laptops into Covert Recording Devices to Monitor WFH', *Australian Financial Review* (online, 24 August 2025) <<https://www.afr.com/work-and-careers/workplace/company-turned-laptops-into-covert-recording-devices-to-monitor-wfh-20250822-p5mp0z>>.
- ¹⁸ Dara Kerr, 'Meta Used AI to Tag Workers Who Took Leave to be Laid Off, Lawsuit Claims', *The Guardian* (online, 15 July 2026) <<https://www.theguardian.com/technology/2026/jul/14/meta-ai-mass-layoffs-lawsuit>>.
- ¹⁹ *Privacy Act 1988* (Cth) s7B(3).
- ²⁰ Human Technology Institute, *Surveillance Creep: Tech-enabled Surveillance of Australian workers* (March 2026) 18 [Table] <<https://www.uts.edu.au/news/2026/03/australian-law-must-protect-workers-from-harmful-tech-enabled-surveillance/contentassets/hti-snapshot-report-worker-surveillance.pdf>>.
- ²¹ Attorney-General's Department (Cth), *Exposure Draft Privacy Amendment (Personal Data Protection) Bill 2026* (August 2026) <<https://consultations.ag.gov.au/rights-and-protections/privacy-reform/>>.
- ²² Explanatory Memorandum, *Privacy Amendment (Private Sector) Bill 2000* (Cth) 5.
- ²³ House of Representatives Standing Committee on Employment, Education and Training, Parliament of Australia, *The Future of Work: Inquiry into the Digital Transformation of Workplaces* (Final Report, January 2025) 58 <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Employment_Education_and_Training/DigitalTransformation/Report>.
- ²⁴ Anthony Albanese, 'AI in Australia's Interests' (Speech, University of Sydney, 15 July 2026) <<https://www.pm.gov.au/media/ai-australias-interests-0>>; Department of Industry, Science and Resources (Cth), *National AI Plan* (2025) <<https://www.industry.gov.au/sites/default/files/2025-12/national-ai-plan.pdf>>; Michelle Rowland, 'AI Consumer Safety Priorities' (Media Release, 20 July 2026) <<https://ministers.ag.gov.au/media-centre/ai-consumer-safety-priorities-20-07-2026>>.
- ²⁵ *Work Health and Safety Amendment (Digital Work Systems) Act 2026* (NSW); Victorian Government, *Response to Legislative Assembly Economy and Infrastructure Committee Inquiry into Workplace Surveillance* (November 2025) <<https://www.parliament.vic.gov.au/4ac989/contentassets/b96fca8977504dbe8c6dfe69dd140007/victorian-government-response---inquiry-into-workplace-surveillance-report.pdf>>; Jacinta Allan, 'Big Tech Must Stop Spying on Workers at Work' (Media Release, 20 July 2026) <<https://www.premier.vic.gov.au/big-tech-must-stop-spying-workers-work>>.
- ²⁶ Sarah Sacher and Edward Santow, Human Technology Institute, University of Technology Sydney, *Submission to the Attorney General's Department Consultation on the Use of Automated Decision-Making by Government 2024* (Submission, 2024), <<https://www.uts.edu.au/globalassets/shared-media/documents/research/hti/hti-submission-use-of-adm-by-government.pdf>>.
- ²⁷ Clare Brennan, Sarah Sacher and Edward Santow, Human Technology Institute, University of Technology Sydney, *Submission to the Senate Community Affairs Legislation Committee inquiry into the National Disability Insurance Scheme Amendment (Getting the NDIS Back on Track No 1) Bill 2026* (Submission, 2026) <<https://www.uts.edu.au/globalassets/shared-media/documents/research/hti/hti-ndis-bill-submission---final.pdf>>.
- ²⁸ Parliament of Australia, *Parliamentary Debates*, Senate, 11 February 2026, 19 (Ms Rachel Blackwood).
- ²⁹ Evidence to the Community Affairs References Committee, Parliament of Australia, Canberra, 1 April 2026, 6 (Robert Day).
- ³⁰ Melissa Davey, "'Stuff of nightmares': calls for help surge 50% after Australia launches aged-assistance tool' *The Guardian*, 24 February 2026 <<https://www.theguardian.com/australia-news/2026/feb/23/calls-for-help-surge-aged-assistance-tool-care-homes-australia>>.
- ³¹ Melissa Davey, 'Labor's controversial algorithm tool for aged care under investigation by Ombudsman' *The Guardian*, 15 April 2026 <<https://www.theguardian.com/australia-news/2026/apr/14/labor-aged-care-algorithm-tool-ombudsman-investigation>>.
- ³² Commonwealth Ombudsman, *Automation in the Targeted Compliance Framework: when the law is changed but the system isn't* (August 2025) 5

<https://www.ombudsman.gov.au/_data/assets/pdf_file/0017/320750/Automation-in-the-Targeted-Compliance-Framework.pdf>.

³³ Joseph Brookes, 'Automated welfare compliance saga hangs over budget' *Innovation Aus* <<https://www.innovationaus.com/automated-welfare-compliance-saga-hangs-over-budget/>>.

³⁴ Jonathan Barrett, 'It doesn't make sense': why recipients of ATO 'robotax' letters are scratching their heads' *The Guardian* (30 November 2023) <<https://www.theguardian.com/australia-news/2023/nov/30/ato-on-hold-tax-debt-letters-robodebt-apology>>; Jonathan Barrett, 'ATO apologises for 'unnecessary distress' caused by on-hold tax debt recovery letters' *The Guardian* (29 November 2023) <<https://www.theguardian.com/australia-news/2023/nov/29/ato-apologises-for-unnecessary-distress-caused-by-on-hold-tax-debt-recovery-letters>>.

³⁵ Commonwealth Ombudsman, *Automated decision-making: Better practice guide* (2019) 10; Australian Human Rights Commission, *Human Rights and Technology* (Final Report, March 2021) 56.

³⁶ Rights to internal review are especially important since most people will not seek external review - e.g. only five out of every 10,000 Robodebts were reviewed by the AAT: 'Unravelling Robodebt: Legal Failures, Impact on Vulnerable Communities and Future Reforms' *University of Sydney* (Web Page) 13 December 2023 <<https://www.sydney.edu.au/law/news-and-events/news/2023/12/13/unravelingrobodebt-legal-failures-impacts.html>>

³⁷ Australian Government, *Government Response: Privacy Act Review Report* (September 2023) <<https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report>>.

³⁸ See, e.g., Daniela Pizzirani and Dannielle Maguire, 'Facial recognition technology 'scope creep' is upon us, experts warn' *ABC News* (Online) 1 September 2026 <<https://www.abc.net.au/news/2026-09-01/supermarket-violence-retail-crime-facial-recognition-technology/107056936>>; Ima Caldwell, 'WA police facial recognition trial launches with a real-time arrest – and backlash over privacy' *The Guardian* (Online) 20 July 2026 <<https://www.theguardian.com/australia-news/2026/jul/20/western-australia-police-real-time-facial-recognition-trial-privacy-ntwnfb>>.

³⁹ See, e.g., Josh Taylor, 'Kmart sells out of low-cost rival to Meta camera glasses across Australia amid warnings of 'privacy nightmare' *The Guardian* (Online) 4 August 2026 <<https://www.theguardian.com/australia-news/2026/aug/04/kmart-camera-glasses-anko-meta-smartglasses-australia>>.

⁴⁰ Dhruv Mehrotra and Dell Cameron, 'Meta Silently Added Face-Recognition Code for Its Smart Glasses to Millions of Phones' *Wired* 4 June 2026 <<https://www.wired.com/story/meta-smart-glasses-face-recognition-nametag-connections/>>.

⁴¹ Nicholas Davis, Lauren Perry & Edward Santow, *Facial Recognition Technology: Towards a model law*, Human Technology Institute, The University of Technology Sydney (Report, September 2022).

⁴² *Privacy Act 1988* (Cth) s7B(3).

⁴³ Australian Law Reform Commission, *For your information: Australian privacy law and practice* (ALRC Report 108, August 2010) [33.44].

⁴⁴ Attorney-General's Department, *Portfolio Budget Statements 2026-27: Office of the Australian Information Commissioner – Entity resources and planned performance* (June 2026) 4 <<https://www.ag.gov.au/system/files/2026-05/2026-27-ag-pbs-oaic.PDF>> IDM, 'Funding Squeeze hits OAIC as Privacy Reforms Land' *Blog Post* (15 May 2026) <<https://idm.net.au/article/0015590-funding-squeeze-hits-oaic-privacy-reforms-land>>.

⁴⁵ Office of the Australian Information Commission, *Corporate plan 2026-27* (August 2026) <<https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/corporate-plans/corporate-plan-202627#section-overview>>.

⁴⁶ *Digital ID Act 2024* (Cth) s 55.

⁴⁷ Commonwealth, *Parliamentary Debates*, House of Representatives, 24 June 2009, 6989 (Craig Anthony Emerson, Minister for Small Business) <https://parlinfo.aph.gov.au/parlInfo/download/chamber/hansardr/2009-06-24/toc_pdf/69153.pdf;fileType=application%2Fpdf#search=%22chamber/hansardr/2009-06-24/0078%22>.