



Drawing the line

Tech-enabled surveillance of Australian workers

About HTI

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.

Authors: Sophie Farthing, Sarah Sacher, Professor Edward Santow and Angus Vos.

HTI expresses particular thanks to Adj Prof Peter Leonard and Peter Lewis, who provided expert review of a draft of this Final Report; Gilbert + Tobin, which contributed legal research under the leadership of the firm's partner, Simon Burns and HTI's AI Policy and Regulation Expert Reference Group for their strategic input. The views expressed in this Report, and any errors, remain the sole responsibility of HTI.



Safe Ai

The work program, under which this Report was created, is proudly supported by the Munderoo Foundation.

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.

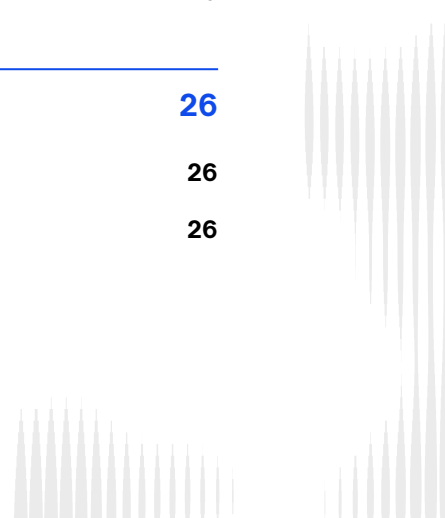
Contents

Executive summary	2
--------------------------	----------

Drawing the line	4
Introduction	4
Tech-enabled surveillance of workers in Australia: Where we are now	5
Tech-enabled surveillance is rising rapidly	5
Surveillance may have a place at work – but employers need to know where to draw the line	7
Australian workers are experiencing harms right now	7
Australian workers are increasingly concerned about intrusive surveillance	9
Law reform is urgent	11
HTI's law reform proposal	12
The path forward: enabling reasonable monitoring and preventing unreasonable surveillance	12
Overview of HTI's proposal	13
Substantive protections: An amendment to the Fair Work Act	13
Accessible complaint handling in the Fair Work Commission	16
Worker surveillance clauses in EBAs and modern awards	16
Clear and practical guidance by the Fair Work Ombudsman	17
Reform must be led by the Federal Government	18

Appendix A	19
Applying the fair and reasonable requirement factors	19
Application to high-risk technologies and contexts	25
Ministerial power to proscribe certain technologies	25
Application to high-risk government operational contexts	25

Appendix B	26
Concurrency	26
Simplification of state and territory laws	26



Executive summary

Rise in tech-enabled worker surveillance

Technology is creating new ways to monitor workers.

Thoughtful monitoring can support well-run, safe workplaces. However, in the age of artificial intelligence (AI), technology is combining with increased flexible and remote working arrangements to create a rising tide of harmful worker surveillance.

Monitoring tools range from bespoke surveillance tech, like facial recognition cameras, 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. 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. This awareness gap is quickly closing. There is growing concern, especially from Australian workers and unions, about unchecked surveillance.

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. And yet our law is complicated, confusing and riddled with gaps. As a result, employers cannot be confident about what lawful worker monitoring entails, and workers are inadequately protected from harmful surveillance.

In this Report, the UTS Human Technology Institute (HTI) outlines the reform needed to address this problem. We propose the Australian Government take the lead by amending employment law to distinguish reasonable monitoring from harmful surveillance.

This Report is the product of deep consultation with workers, employers and experts. HTI's March 2026 Snapshot Report, *Surveillance Creep*, described the rise of tech-enabled worker surveillance, and set out our preliminary views regarding reform. In the months since, HTI has tested and refined this proposed reform, in consultation with unions, industry groups, legal experts and government stakeholders.

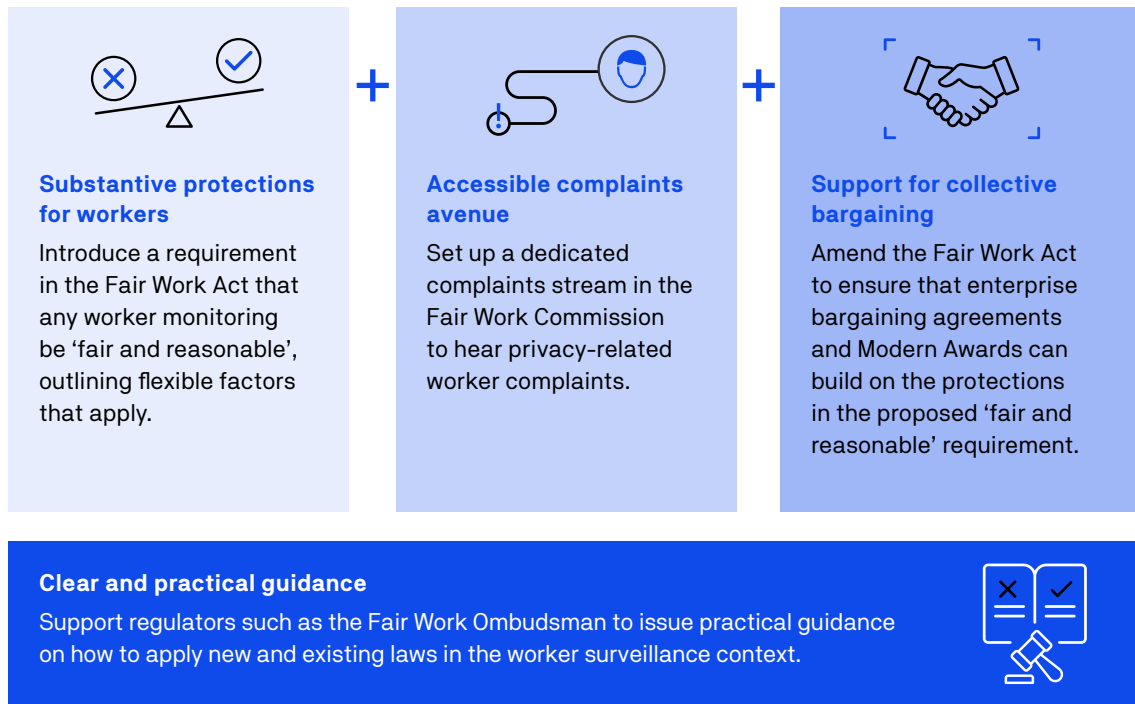
There was broad agreement among stakeholders representing workers and employers that our current law is failing. Workers lack crucial protections from surveillance-related harms. At the same time, employers are unclear on when and how they can monitor their workers. There is a strong impetus for reform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

Worker monitoring should be fair and reasonable

The centrepiece of HTI's proposed reform is to introduce in the *Fair Work Act 2009* (Cth) a requirement that any worker monitoring be 'fair and reasonable'. This requirement would build on the Albanese Government's commitment, now set out in the Exposure Draft Privacy Amendment (Personal Data Protection) Bill 2026, that personal information generally should be handled fairly and reasonably.

HTI's proposed reform to the Fair Work Act would allow workers to have complaints about unreasonable or harmful surveillance heard by the Fair Work Commission, and it would also provide for more detailed, workplace-specific requirements to be addressed in enterprise bargaining agreements and modern awards. In addition, the regulator should provide guidance for employers on how to fulfil their obligations in this area.

Key reform proposals



Federal leadership is needed for this urgent and important reform

The Australian Government has a clear mandate to undertake this reform, 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'. 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 that can be kicked down the road. 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 NSW and Victorian Governments have recognised the urgency of the problem and have independently initiated reform processes. 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.

Drawing the line

Introduction

Worker monitoring is rapidly increasing in Australia – fuelled by new technology like AI. While some monitoring is legitimate, too much is unreasonable and harmful.

This problem is not addressed by our law, which is 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.

The recommendations outlined in this Report would:

- improve the human rights protections of workers in relation to technology-enabled surveillance, especially as AI transforms how Australians work; and
- clarify the law so that employers better understand what forms of worker monitoring and surveillance are lawful and unlawful.

This Report outlines the rise of tech-enabled worker surveillance, incorporating new research on Australian worker attitudes. It then sets out how Australian law should be reformed to better enable safe and appropriate worker monitoring, while addressing the harms caused by unreasonable worker surveillance. HTI's reform recommendations have been thoroughly tested with: unions and other civil society organisations; industry bodies; privacy, employment and other relevant experts; and government stakeholders.

Definition of tech-enabled worker surveillance

Technology-enabled worker surveillance refers to the use of technology to monitor workers for the purposes of managing and influencing their behaviour or making workplace decisions.¹ This involves the collection and use of data about workers, including workers' activities; location and movements; oral or written communications; biometrics; personal characteristics and behaviour; facial expressions or physical state; and online activity or device usage.²

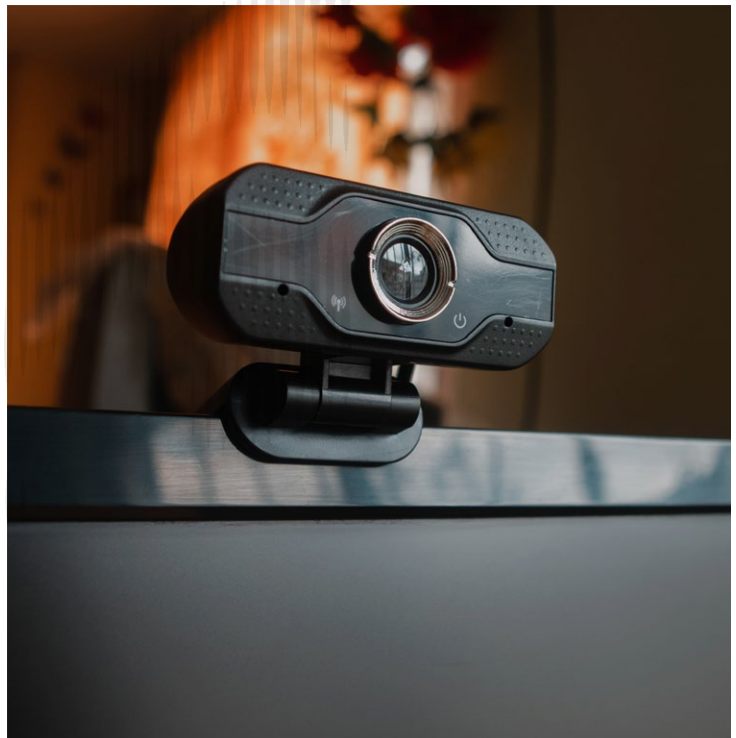
Technology-enabled monitoring tools include AI-powered products and services (for example, email tracking), and other technologies (for example, CCTV and audio-recording devices). AI-powered tools often use personal data to assess or profile individuals. They can be used to evaluate worker performance, which can in turn be used in automated or AI-informed decisions about workers,³ including regarding hours, pay, leave, task allocation, hiring, promotions, disciplinary actions and termination.

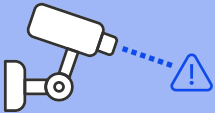
Tech-enabled surveillance of workers in Australia: Where we are now

Tech-enabled surveillance is rising rapidly

With the rise of AI and other technology-enabled tools, monitoring of workers has become more widespread and now covers a greater array of aspects of workers' professional and personal lives. This reflects a growth in inexpensive, bespoke surveillance tools as well as in tech products and services that have embedded surveillance capabilities. In parallel, trends towards remote work have driven demand for, and investment in, worker surveillance technology. New AI capabilities are expanding the scale and intrusiveness of surveillance, and opening up new frontiers for monitoring – including in workers' homes, and via their bodies and emotions.

Tech-enabled surveillance tools are being adopted across a range of work contexts – from factory floors, to retail stores, to truck fleets, to law offices. Types of surveillance tools are set out in the infographic below.



Focus of surveillance	Online and on-device activities 	Physical location, movement and breaks 	Verbal communications 
Types of tools	■ Keystroke monitoring and screen capture tools ■ Internet monitoring and filtering ■ Monitoring of email and instant messaging ■ Social media analytics ■ Cloud-based software measuring and analysing engagement (eg, time spent online)	■ Wearable tracking devices ■ Desk sensors ■ GPS monitoring via smartphone apps or work vehicles	■ Audio-recording via wearables or laptops ■ Call recording and analysis ■ Voice assistant recording
Focus of surveillance	Visuals 	Biometrics 	Emotion, attention, attitude and physical state 
Types of tools	AI-enabled webcams, CCTV or body cameras which can identify people or objects and track movement	■ Fingerprint scans ■ Facial recognition technology ■ Retinal scans	■ Wearable neurotechnology ■ AI tools that assess facial expressions and vocal tone to infer emotions ■ LLM sentiment analysis tools that analyse written communications for tone and attitude ■ Smartwatches that monitor and assess health data

Surveillance may have a place at work – but employers need to know where to draw the line

Employers adopt monitoring tools for a range of reasons. Often, they simply wish to know, and influence, what workers are doing.⁴ Other common motivations include: optimising productivity; improving worker performance; protecting work health and safety; protecting cybersecurity, including conducting identity verification; and protecting work property. Monitoring data about workers can also be used for secondary purposes such as training AI models.⁵

These monitoring tools can also be unreliable or even counterproductive. Unreasonable surveillance can reduce performance, drive staff turnover, prompt rule-breaking, and damage trust between workers and employers.⁶ Many monitoring tools are simply ineffective at measuring and improving productivity in meaningful ways – for example, tools that measure the number of emails a worker sends, or meetings they attend, do not necessarily reveal anything about the worker's productivity or their work quality.

Australian workers are experiencing harms right now

Unreasonable surveillance can lead to a range of harms to workers individually and to the broader Australian workforce:

- **Privacy and blurred lines between work and home life:** tech-enabled monitoring tools can cause harm by exposing personal information that is entirely unrelated to a worker's job – such as data about their sexuality or beliefs.
- **Accountability and access to information:** surveillance can increase information asymmetries between employers and workers, with systemic effects across workforces – inhibiting the exercise of workplace rights.
- **Human dignity:** workers often feel dehumanised by relentless, punitive scrutiny and micro-management by machine.
- **Work health and safety risks:** unreasonable surveillance is linked to stress, mental health issues, physical injuries, and workplace accidents.
- **Bias, discrimination and exclusion:** some technology-enabled monitoring tools can produce higher rates of error for certain groups (for example, women, young people, and people with a disability), and this can increase the risk of discrimination or unfairness for those groups.
- **Freedom of expression and association:** the fact or threat of being watched can prevent workers from joining a union, or speaking and moving freely – including outside the workplace.

There have been several high-profile examples of tech-enabled surveillance causing harms to Australians. These include Woolworths' 'framework', which was a factor contributing to the 2024 Woolworths strike.⁷ 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.

Another example is the Safetrac case, where a Victorian company used work-issued laptops to record audio of staff working from home for up to eight hours a day, without their knowledge or consent.⁸ The software was capable of capturing private conversations within families, and confidential information discussed with clients.⁹ This highlights the level of intrusion of some employers into the home and family lives of remote workers.

Recently, the Finance Sector Union has raised concerns about the Commonwealth Bank's 'Navigate' app. Workers are required to download the app, which is used as a pass for office entry and tells employers when workers are in the building. The app continuously collects data on workers' locations and can connect to any Bluetooth device while workers are working from home.¹⁰

Worker surveillance used to train AI and identify workers for dismissal

A recent lawsuit alleges that Meta used data from performance rankings, and keystroke and activity-monitoring data, to target workers for mass layoffs. The claimants say that Meta used AI to 'score, rank and select' employees for exclusion.

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 and other forms of approved leave received a lower rating – in some cases resulting in discrimination.¹¹

Ahead of these layoffs, Meta had also reportedly begun tracking mouse movements, clicks and keystrokes as data to train future AI agents.¹² Some describe this practice as turning workers into vehicles for training their replacements.¹³

Beyond the headlines, data collected by unions and evidence to Australian inquiries, as well as anecdotal information provided to HTI through the consultation process, highlight the depth of the harms currently experienced by Australian workers.

Experiences of Australian workers

- The Australian Workers Union documented the introduction of a productivity tool in a warehouse distribution centre: *'this is affecting [workers'] mental health in really serious ways. People are talking about sitting in their car having panic attacks before going to work, being medicated because of the job... Members [have talked] about it making them feel suicidal... We have [heard] how dehumanising it is to be monitored second to second, to have their toilet breaks monitored, and just how they feel very resentful and often very ashamed.'*¹⁴
- A legal service provider reported that a worker was told their workplace had a 'no tracking policy' related to vehicles, and yet the worker was later dismissed based on data obtained through vehicle tracking. The worker was not provided with the data that formed the basis of the allegations.¹⁵
- The Victorian Trade Halls Council reported that a young worker was *'required to be on Zoom every hour she was working, even while she was on the phone or drafting material, so her employer could watch her work. Her manager separated her out into breakout rooms and used the rooms to sexually harass and bully her... She found the constant surveillance extremely intimidating and left her job without having another one lined up'*.¹⁶

Australian workers are increasingly concerned about intrusive surveillance

Australian employers have reported significant use of surveillance tools. For example, a 2021 employer survey found 91 percent of Australian employers monitored their remote workers' locations through software.¹⁷

However, workers themselves have low awareness of the true extent of worker surveillance, even when they are directly affected. A March 2026 poll, commissioned by the Minderoo Foundation, found 43 percent of over 2000 Australians surveyed were aware that some employers use technology (including AI) to monitor workers. Only 9 percent knew that monitoring was used in their *own* workplace.¹⁸

This highlights a significant awareness gap – but the gap is quickly closing. Workers are becoming increasingly concerned about surveillance. As one senior union representative told HTI, this issue is 'widely and deeply felt across the union movement'.

There is growing support for stronger regulation. A Redbridge survey of 1,507 NSW workers in 2026 found that 69 percent of workers support tougher regulation of AI in workplaces, including limits on invasive surveillance.¹⁹ The Tech Policy Design Institute has found that 85 percent of Australians surveyed support regulation of AI, with reform in workers' rights a key priority of those surveyed.²⁰

In June 2026, the Minderoo Foundation commissioned Talbot Mills to explore Australian worker attitudes towards surveillance through six focus groups, building on polling conducted in March. Workers expected stronger legal protections from some forms of surveillance than currently exist. Below are some key themes emerging from the research.



Worker attitudes: findings from quantitative and qualitative research²¹

Acceptance of monitoring is context dependent

75 percent of workers in the quantitative polling agreed that monitoring should be used only where it is clearly communicated and strictly necessary to check they are meeting their job requirements. Similarly, workers felt that punitive forms of monitoring undermined trust, dignity and fairness in the workplace.

Trust is a two-way street

Where monitoring signalled that an employer did not trust their employees, workers judged it to be unreasonable, almost regardless of the technology used. For example, in response to a scenario about employers tracking worker breaks, a participant commented that 'you should be innocent until proven guilty... to immediately think that you are guilty until proven innocent is not really fair'.

Workers have strong concerns about intrusive forms of surveillance

This qualitative research reinforced polling which found workers are highly concerned about audio surveillance (72 percent), live-screen monitoring (71 percent), location tracking (71 percent), and emotion recognition (70 percent). Workers viewed things like audio-recording and live-screen recording as 'spying' and 'a bit like Big Brother.' One stated that without a serious and legitimate reason, the use of intrusive methods like remotely activating microphones was 'completely unreasonable... ridiculous and illegal.' Another said, 'if you can't manage your staff without spying on their home life, you're a pretty rubbish manager'.

Workers are sceptical about the fairness of productivity tools

AI-generated productivity metrics with penalties attached were seen as unfair and blunt, as well as discriminatory towards older workers and people with disability. One participant commented 'we're not robots... I don't think it is fair at all... there were 60-year-olds doing what I was doing at 25'. Others questioned the effectiveness of such tools, commenting, 'you're asking an employee to pretend that they're working' and 'are they looking for quality or quantity here?'.

Consent is necessary, but not sufficient

While obtaining the consent of workers was seen as important, it did little to mitigate concerns about more invasive practices which many participants felt cross a fundamental line regardless of what was formally agreed. Some noted that providing consent under the threat of losing your job is not a real choice.

Law reform is urgent

The Australian laws that govern worker surveillance are complex, confusing and contain important gaps. These include federal, state and territory privacy laws; state and territory general and workplace-specific surveillance laws; as well as federal, state and territory work health and safety laws.

At the federal level, workplace laws do not directly regulate worker surveillance, and the *Privacy Act 1988* (Cth) 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. 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. Another problem is that they focus on the use of specified ‘devices’, rather than acts or practices of surveillance – this makes them outdated and difficult to apply, as they do not adequately take into account new technologies such as AI.

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.

Legal issue relating to worker monitoring	Federal Privacy Act	State and territory general surveillance laws	NSW and ACT workplace surveillance laws
Protections against surveillance in certain areas like bathrooms, change rooms	✗	—	✓
Other protections regardless of a worker’s purported consent	✗	✗	✗
Specific consideration of workers and the workplace context	✗	✗	✓
Extension of protections to workers and workplace data	—	✓	✓
Protections against intrusive monitoring of workers’ personal data and activity on computers or other devices (“data surveillance”)	—	—	✓
Regulation of the collection and use of biometric information	—	✗	✗
Regulation of new AI-driven tools, such as emotion recognition tools, productivity tools and neurotechnology	?	?	?
Articulation of protected ‘private activities’ and ‘private conversations’ applicable to modern ways of working	✗	?	?
	Work health and safety laws	Fair Work Act	Anti-discrimination laws
Application of existing obligations to new AI tools	?	?	?
Clarity regarding liability for workplace decisions made or directly informed by AI tools owned or managed by third parties	?	?	?

Key:

- ✗ No regulation or protection
- ✓ Regulatory coverage/protection
- ? Uncertain regulation/protection
- Incomplete regulation/protection

HTI's law reform proposal

The path forward: enabling reasonable monitoring and preventing unreasonable surveillance

HTI's approach to law reform is underpinned by five key principles.

The law should make clear when worker monitoring is, and is not, lawful. While it may be reasonable for an employer to monitor workers appropriately for safety and other similar reasons, too often worker surveillance goes well beyond this. In relying on fictitious consent, our laws do not set clear boundaries or 'red lines' that would prohibit unreasonable surveillance.

This leaves workers vulnerable to harm. Employers also often don't know what they can and can't do. Law reform should articulate the line between reasonable monitoring and harmful surveillance. A balanced approach would consider the employer's legitimate interests and obligations, and workers' human and legal rights.

Law reform should be adaptable to new technologies so that it remains applicable into the future. A technology-neutral approach would ensure a regulatory focus on the harms associated with the use of these tools. This can be achieved through the articulation of flexible principles that apply to a range of technologies, types of workplaces, and workplace scenarios.

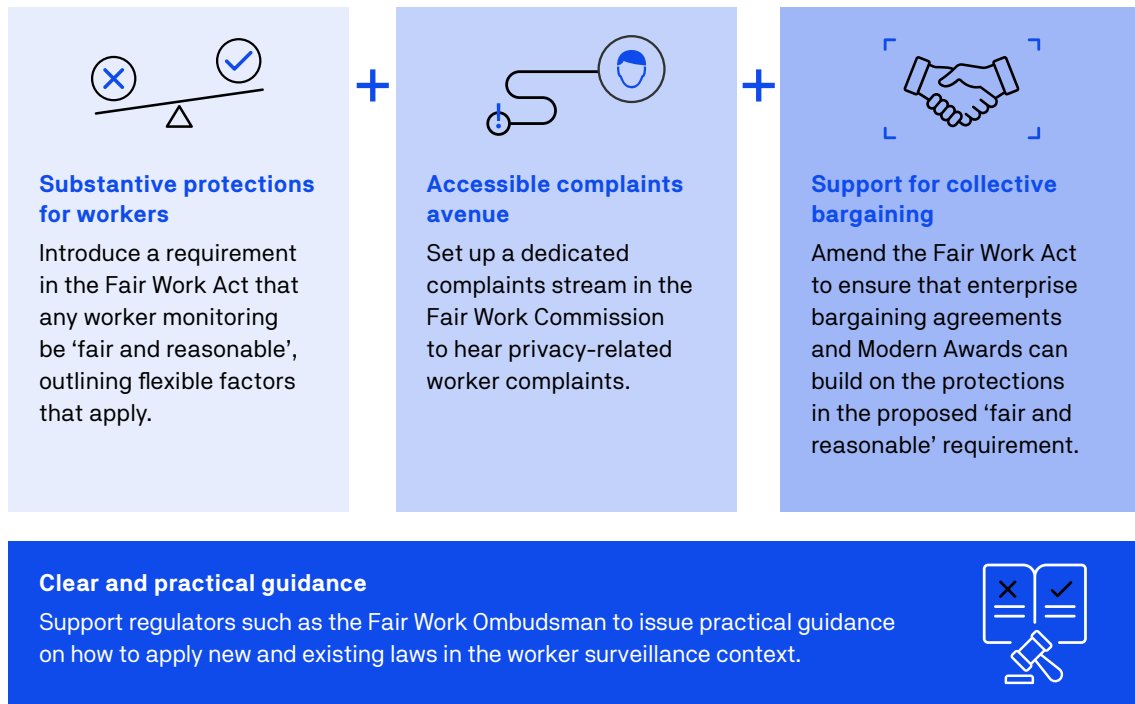
Reform should harmonise and simplify existing laws, rather than adding to the existing regulatory complexity. This goal can also be supported through practical regulatory guidance to provide certainty and support effective compliance.

Law reform should support collective bargaining. Our workplace laws recognise the importance of collective bargaining in navigating the rights and interests of workers and employers. Reform should set clear high-level rules, with more specific guardrails set via collective bargaining in particular industries and workplaces.

Reform should be practical and readily implementable. It should address key harms and gaps in the law, without a prolonged reform process. This would not negate the possibility of future reforms to comprehensively address the full range of issues that may arise in this space, such as reforms to anti-discrimination laws.

Overview of HTI's proposal

As outlined below, HTI recommends the following law and policy reform.



Substantive protections: An amendment to the Fair Work Act

A requirement that any worker monitoring be 'fair and reasonable'

HTI's primary recommendation is for the Australian Government to introduce into the *Fair Work Act 2009* (Cth) a requirement that any worker monitoring be 'fair and reasonable'. This new requirement regarding the collection and use of personal information about workers would be articulated in law, and it would be accompanied by regulator guidance. In practice, the reform would draw a clear line between reasonable monitoring of workers, and unreasonable surveillance.

The Australian Government has already committed to introducing a more 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 Privacy Amendment (Personal Data Protection) Bill 2026.²² This would be an important and welcome reform, as it would set minimum standards for personal data collection and use even where an individual purportedly consents to the data handling.

However, the Privacy Act largely does not apply in this employment context, because of the ‘employee records’ exemption. Hence, HTI recommends that this committed reform be applied in the more specific context of conduct regulated by the Fair Work Act. The factors that determine whether an action is fair and reasonable have been comprehensively tested through the Privacy Act review process,²³ and HTI has further tested and outlined how these factors may be practically adapted for the workplace.

This reform to the Fair Work Act would address the problem that workers often cannot provide genuine, free and informed consent to the handling of their personal information.

Fair and reasonable requirement factors

Factor	Example
Is the 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 proportionate 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.

A ‘fair and reasonable’ requirement in the Fair Work Act could be applied to a broad range of workplace contexts, balancing legitimate employer and worker rights, interests and obligations. The factors draw on international human rights law, with similar laws already adopted in jurisdictions such as the European Union and the United Kingdom.²⁴ This reform would, therefore, make Australian law more interoperable with those laws, thereby helping to minimise the regulatory burden on companies operating across multiple international jurisdictions.

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’.²⁵ 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.

While the proposed ‘fair and reasonable’ requirement would set the general rule, the Minister also should have the power to proscribe certain surveillance products and services that pose an unacceptable risk to workers’ human rights. The exercise of this power should be subject to public consultation and input from relevant regulators. This would enable the Government to address community concern where a particular tool, product or service is deemed too high-risk for workplace adoption, whether in the short term (for example, until it is deemed safe for use) or the long term. For example, several ministers have reflected on community concern about the use of ‘smart glasses’, which are equipped with AI-powered cameras capable of capturing and analysing audio and visual material.²⁶ Such concern is likely to be particularly strong in a workplace context, as smart glasses could be used to covertly surveil workers. A ministerial power to address concerns with specific products and services, such as smart glasses, would allow risks to be addressed in this fast-moving area of technological development.

A detailed analysis of how the ‘fair and reasonable’ requirement factors would apply is set out in **Appendix A**.

The Fair Work Act as the home of worker surveillance protections

HTI tested several options for ‘housing’ worker surveillance protections, including via reform to the Fair Work Act, the Privacy Act and the Model Work Health and Safety Act. While reforming any of these instruments would be viable, HTI’s conclusion is that amending the Fair Work Act would present the best and most straightforward option.

Stakeholders consulted by HTI generally preferred reform to the Fair Work Act, because this statutory regime is well understood by employers and workers. The Act protects a wide range of workers’ rights, balancing worker and employer interests. It also has established processes for collective bargaining and dispute resolution that can accommodate worker surveillance issues.

Relatedly, there are benefits associated with worker surveillance issues being governed by a well-established and accessible regulator in the Fair Work Commission. This would enable the consideration of worker surveillance issues at the main ‘point of impact’ for workers: namely, where surveillance data has influenced decisions about a worker’s legal rights or interests, such as adverse action or dismissal.

Regardless of where the primary reform is implemented, consequential amendments can address overlaps between legislative regimes at the federal and state levels. Additionally, regulatory guidance would help employers understand how the law applies.

Scope of the fair and reasonable provision

The fair and reasonable requirement would encourage employers to engage in an open dialogue with workers about the monitoring they plan to use. This is likely to improve the quality of consent that employers obtain from their workers if they do opt to use monitoring or surveillance.

The fair and reasonable provision should be tied to ‘workers’ data, rather than ‘workplaces’. The term ‘worker’ is broadly defined in section 12 of the Fair Work Act.²⁷ It includes traditional employees (where there is a formal employment contract between the worker and their employer), as well as less formal relationships, where an individual performs work for an organisation, often without a formal employment agreement. This second category includes gig workers and other independent contractors. Regardless of the sort of worker, the proposed reform would apply wherever work takes place: in traditional workplaces, and where work is conducted from home, off-site or from a vehicle.

To avoid any doubt in its interaction with the Privacy Act, the proposed reform to the Fair Work Act should expressly permit oversight of employee records where data about workers is being collected or used for monitoring purposes.

Accessible complaint handling in the Fair Work Commission

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*.²⁸

This proposal would involve the Office of the Australian Information Commissioner (OAIC) and the Fair Work Commission having joint jurisdiction over privacy matters. Such arrangements between regulators are well understood. For example, the Fair Work Commission regulates workplace discrimination and sexual harassment alongside the Australian Human Rights Commission, and the Australian Consumer and Competition Commission shares some jurisdiction with the OAIC in relation to the Consumer Data Right.²⁹

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.

As the Attorney-General's Department Review of the Privacy Act observed when considering the prospect of enhancing privacy protections through the Fair Work Act, the regime is 'accessible to employers and employees and their representatives as a no costs jurisdiction with a focus on informal dispute resolution'.³⁰

Worker surveillance clauses in EBAs and modern awards

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.

This reform would involve amending Part 2-4, Division 5, and Part 2-3, Division 3, Subdivision C of the Fair Work Act, which cover terms that must be included in EBAs and modern awards respectively, to introduce a new requirement to include a worker surveillance consultation clause. The content of a model clause could build upon existing model consultation clauses for enterprise bargaining agreements set out in Part 2-4 of the *Fair Work Regulations 2009* (Cth).

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. For example, in the mining industry, location tracking while on site would likely be considered reasonable due to the safety imperative, but this argument does not apply to workers in a bank – these kinds of nuances could be articulated through negotiated clauses.

Negotiated worker surveillance clauses would be restricted from undermining the minimum protections outlined in the fair and reasonable test. This would align with existing approaches to required clauses in the Fair Work Act. 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 by the Fair Work Ombudsman

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.

Targeted guidance on the practical application of the fair and reasonable factors would help support compliance, particularly for smaller employers. Regulatory guidance can also clarify how different legal regimes intersect with worker surveillance, and help employers to streamline their compliance processes. Such guidance is also useful for workers and unions, as it will assist them to understand and enforce their rights.



Reform must be led by the Federal Government

The Australian Government has put workers at the centre of its National AI Plan. In his landmark speech on AI in July 2026, Prime Minister Albanese emphasised the Government's work on navigating 'AI's role in the workplace', and this has been reflected in AI safety in the workplace being one of the Government's five top AI consumer safety priorities.³¹ The 2026 Australian Labor Party Draft National Platform states that Labor will consider 'whether existing regulatory frameworks are adequate to protect workers from intrusive surveillance' and 'how to ensure that employers remain responsible and accountable for critical decisions, and that the use of AI and automation in the workplace is safe and lawful'.³² These important commitments should now be transformed into action.

Harmful worker surveillance is a nationwide problem, necessitating a national response. HTI's research clearly demonstrates that workers expect the Australian Government to protect them. As AI evolves, and as unions increasingly activate in response to worker concerns, the need for law reform will only become more pressing.

As this Report makes clear, our existing laws are not fit for purpose. A federal response can set overarching protections, and coordinate to ensure regulatory certainty and harmonisation across intersecting legal frameworks. This can be done through targeted amendments to existing technology-neutral laws – something that reflects the Government's preferred approach to AI-focused reform, as outlined in the National AI Plan.

In the meantime, momentum for reform is building in the states and territories – recently, the NSW Government passed the *Work Health and Safety Amendment (Digital Work Systems) Act 2026* (NSW) which extends work, health and safety obligations to AI and digital systems that allocate work. Separately, the Victorian Government has committed to introducing legislation to address a range of worker surveillance harms.³³

Unless the federal government legislates for all Australians, states will continue to take the initiative to protect workers independently – which would result in further regulatory fragmentation. This would compound legal complexity and lead to greater compliance headaches for businesses operating across multiple jurisdictions, as well as inconsistent protections for workers.

A fair and reasonable requirement in the Fair Work Act would provide a basis for regulatory consolidation and harmonisation. Two steps are needed in this regard:

- The proposed fair and reasonable requirement is designed to operate concurrently with existing state and territory laws. This requires consultation with states and territories, and should be expressed in the drafting of the relevant provision.³⁴ Presently only two states have dedicated worker surveillance laws – with both overdue for reform – providing strong impetus for the adoption of consistent federal protections.
- This is an opportunity to adopt a consistent standard for consent and notification processes. A straightforward option would be to align existing laws to the highest standard for consent – namely, the *Workplace Privacy Act 2011* (ACT), or proposed Victorian reforms.

See **Appendix B** for further detail on these points.

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. Workers who are treated with trust and respect are in turn incentivised to work well – with benefits extending far beyond what an AI tool is capable of assessing. If we get these basics right, Australia can weather the storm of technological change and uphold our core values.

Appendix A

This appendix explains in greater detail how the factors for a ‘fair and reasonable’ requirement can be adapted from the privacy law context, to be applied in the Fair Work Act. This appendix also addresses the situation of high-risk contexts and technologies.

Applying the fair and reasonable requirement factors

As previously noted, the Government has released an Exposure Draft for forthcoming Privacy Act amendments, which would introduce a ‘fair and reasonable’ provision in the Privacy Act.³⁵ The Government has identified seven factors or criteria that will assist in determining whether the handling of personal information meets the requirement that the organisation act fairly and reasonably. See the box below. These factors are based on commitments made in the Government’s response to the Attorney-General’s Department Privacy Act Review Report.³⁶

Applying those factors to the more specific context of worker monitoring and surveillance will benefit from some brief elaboration in the Fair Work Act and in regulator guidance.

Fair and reasonable test (Privacy Act Exposure Draft)

An entity must have regard to the following matters in determining whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances:

- a. whether the collection, use or disclosure of the information relates to one or more of the APP entity’s [covered by the Privacy Act – ie, an “APP entity”] functions or activities;
- b. whether a reasonable person would expect the collection, use or disclosure of the information in the circumstances;
- c. whether the APP entity is transparent about the means and the purposes of the collection, use or disclosure of the information;
- d. whether the purpose for which the information is being collected, used or disclosed could be met by collecting, using or disclosing less information, or information that is not personal information;
- e. whether the individual to whom the information relates is provided with genuine choice in relation to the collection, use or disclosure of the information;
- f. the impact on the privacy of the individual to whom the information relates, and any risk of harm to the individual, arising from the collection, use or disclosure of the information (including whether that impact or risk of harm is proportionate having regard to any benefits to the individual or the APP entity arising from the collection, use or disclosure);
- g. if the individual to whom the information relates is a child—the best interests of the child as a primary consideration.³⁷

As outlined below, HTI proposes how these fair and reasonable factors could be adapted and applied to the Fair Work Act context. All of the factors would need to be considered in determining whether the monitoring is fair and reasonable.

Factor (a): Whether the collection, use or disclosure is reasonably necessary for a private sector organisation, or directly related to a government agency's functions and activities; and

Factor (d): Whether the purpose for which the information is being collected, used or disclosed could be met by collecting, using or disclosing less information, or information that is not personal information

Drafting of factor (a)

In its response to the Privacy Act Review Report, the Government committed in principle to factor (a); however, the drafting of this factor has been significantly changed in the Exposure Draft, as compared with the AGD's prior report. The original drafting required consideration of 'whether collection, use or disclosure of information is *reasonably necessary* for a private sector organisation, or *directly related* to a government agency's functions and activities.'³⁸ The Exposure Draft would require merely that the collection, use or disclosure '*relates to one or more*' of an entity's functions or activities.

The Exposure Draft wording is inconsistent with the Government's existing commitment, and would significantly water down the fair and reasonable requirements if adopted. HTI therefore recommends that the original drafting of this factor be adopted in both the Privacy Act, and in the related Fair Work Act provision. The below analysis explains how the preferred articulation would apply in practice.

Application of factors (a) and (d)

Factor (a) is likely to be the first considered for any monitoring activity.

It imposes an objective requirement that the monitoring be reasonably necessary for the organisation. It recognises that employers have a broad but finite range of legitimate purposes for monitoring workers. Monitoring cannot be justified solely on the basis that an individual is 'at work' or 'on work time'.

An employer would need to identify a specific legitimate purpose for the monitoring activity. Examples of legitimate purposes include: to meet safety requirements or other legal obligations, to secure company property, or to check that workers are meeting specified job requirements. Examples of illegitimate purposes are likely to include determining a worker's religion or their sexual orientation. Monitoring workers for the sake of 'keeping an eye on them' or for vague productivity purposes, would not be sufficiently specific.

Having established a legitimate purpose, the monitoring would need to be reasonably capable of achieving the stated purpose. This means that an employer would need to be able to explain how the monitoring activity is likely to be effective in achieving the purpose. For example, if an employer's purpose is to ensure that cyber-security requirements are met on laptop devices, it would not be reasonable to place cameras in company cars, as that is disconnected from the purpose. Similarly, monitoring a worker for their entire work day, inclusive of breaks, would go far beyond what is necessary to achieve any legitimate purpose.

Any monitoring or use of personal data for secondary or other unstated purposes would not be legitimate. Additionally, the choice of monitoring tool, the extent and intrusiveness of the monitoring, and the degree of data collection must be no more than what is reasonably necessary to fulfil the stated purpose. These considerations integrate with factor (d) which requires consideration of whether the purpose could be achieved through less privacy intrusive measures, including by collecting or using less personal information. Employers would be expected to develop and execute data minimisation and deletion policies to comply with this criterion.

The relevant test is ‘whether a reasonable person who is properly informed would agree that the collection, use or disclosure is necessary.’³⁹ The factor would be applied in a practical way. An employer would be expected to consider alternatives to monitoring, or other less intrusive monitoring options. If multiple options are available, an employer would be expected to adopt one that is less, rather than more, intrusive in its practical impact on workers. For example, if an employer wanted to record the days that workers spend at the office, adopting location tracking would be unnecessary, because there are less intrusive options available to achieve the same outcome (like a sign-in system).

The term ‘reasonably necessary’ is not a test of *absolute* necessity.⁴⁰ The employer would not need to show that the sole means of achieving the legitimate purpose is through the chosen monitoring – this approach is consistent with human rights and privacy law standards. Having said this, the more rights-intrusive or potentially harmful the chosen approach, the more stringently the necessity test should apply.⁴¹ This approach is suitable for a test that is intended to apply to a broad range of purposes and circumstances, and it allows for some flexibility in the balancing of rights to be undertaken.

Example: Secondary data use

An employer installs AI-enabled cameras overseeing a construction site, to flag potential safety hazards. It would not be reasonable to use the data collected from this tool to assess the performance of construction workers.

Factor (b): Reasonable expectations of the affected worker; and

Factor (c): Whether the organisation is transparent about the means and the purposes of the collection, use or disclosure of information

Factor (b) involves considering whether a hypothetical worker, acting reasonably in the circumstances of the particular employment arrangement, would expect the particular monitoring measures.

For example, a reasonable person would have a higher expectation of privacy when they are in their own home, as compared to a typical workplace.⁴² Similarly, a worker is likely to expect their employer to monitor their work activities and outputs, but may not expect monitoring to extend to their personal lives, such as their relationships and political beliefs. A worker is also unlikely to expect personal data collected at work to be used for purposes entirely unrelated to work – like for sale to third parties for commercial use. Nor would they expect data to be collected about them outside of ordinary work hours.

Factor (b) interacts with factor (c) which takes into account the extent to which an organisation has been transparent about collection or use of personal data. In the workplace context, the kind and quality of consent processes, notice and policies provided by an employer are all important standalone considerations, which will also influence what workers may reasonably expect.

Example: Remote monitoring of workers

Remote workers would not reasonably expect their employer to collect data about communications they have in their homes, which are not work-related. They would not expect data about their family members or communications of those family members to be collected. They similarly would not expect to be monitored while taking breaks in their private space.

Factor (e): whether the individual to whom the information relates is provided with genuine choice in relation to the collection, use or disclosure of the information

As noted above, the fair and reasonable requirements do not negate the importance of obtaining genuine consent. If an employer has complied with consent requirements at the state and territory level, this should be considered adequate for the purposes of the federal test.

Factor (f) Risk of harm to the individual, and proportionality assessment

This factor reflects the well-established international human rights law proportionality test, and requires the consideration of a number of key questions that build on considerations in previous factors.

What is the likelihood of adverse impact on workers?

This involves consideration of what legal or human rights may be interfered with, such as privacy, non-discrimination or worker rights protected under workplace laws.

It also involves assessing the severity of the possible impact on rights. The more severe the impact on rights, the less likely the surveillance will be legitimate. For example, audio-recording is a strong invasion of privacy, while monitoring the amount of time a worker spends logged into a work system is less severe. The former may not be legitimate without a very strong justification and rigorous safeguards, while the latter may be more readily justifiable.

Are certain groups particularly at risk, or likely to experience disproportionate impacts?

This involves consideration of groups who may experience distinct or compounded adverse impacts as a result of the adoption of a monitoring tool. Employers should pay specific attention to whether groups with protected attributes under anti-discrimination law may be unduly disadvantaged. For example:

- a warehouse productivity tool that does not take into account reasonable accommodations for people with disability will disproportionately impact that group
- an on-device tool that measures how productive a person is within work hours may mischaracterise the productivity of workers with flexible work arrangements, disproportionately affecting workers with caring responsibilities
- an emotion-recognition tool trained on data from the general population may have significantly higher inaccuracy rates for people from culturally or linguistically diverse backgrounds, or neurodiverse cohorts.

What kind, sensitivity and amount of worker data is being handled by the employer?

Almost every employment relationship involves some collection of personal data. However, when such data is collected, there should be protections in place to secure the data; and to prevent unnecessary, excessive data collection beyond what is required for the employer to meet their business and legal requirements. There should be a strong justification where employers want to collect and rely on sensitive data, such as biometrics, to monitor workers.

For example, where a company wishes to use facial recognition technology there should be a strong justification for its adoption, such as heightened or sensitive workplace security risks. There should also be strong data governance processes, including a dedicated privacy policy and technical safeguards to ensure that biometric data is not misused – for example, ensuring that worker data is held no longer than is necessary to complete an identity verification process.

Are there safeguards in place to mitigate potential harms?

Strong safeguards around the use of monitoring tools can mitigate harms to workers. Safeguards may include routine audits of monitoring tools to ensure accuracy; requirements for management to personally review AI-informed decisions, and for employees to provide input and challenge AI-informed decisions; and strong data governance policies to prevent purpose-creep and misuse of employee data.

Factor (g): if the individual to whom the information relates is a child—the best interests of the child as a primary consideration

This factor reflects the need for additional protections for workers under the age of 18, due to their particular vulnerabilities. As recognised by Safe Work Australia, young workers are at greater risk of exposure to both physical and psychosocial hazards at work,⁴³ and research indicates that this vulnerability extends the range of harms associated with worker surveillance.⁴⁴

The Australian Government recognised the need for dedicated protections for the use of children's data when it amended the Privacy Act to provide for a Children's Online Privacy Code (the Code) to be developed by the OAIC.⁴⁵ The Exposure Draft of the Code sets out additional requirements related to the use of children's data, including consideration of their best interests.⁴⁶ The considerations in the Code, while not applicable to the workplace context, would nonetheless be readily transferable to this factor.

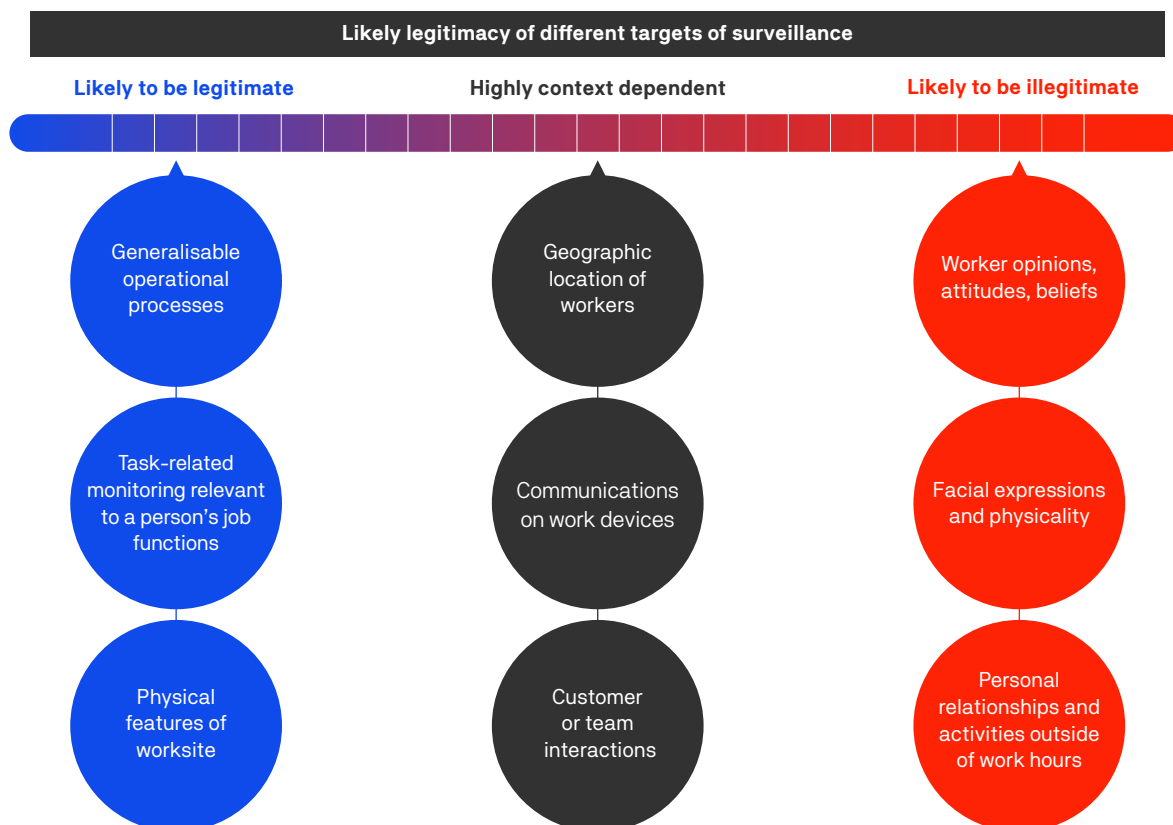
When applying this factor, employers that employ young workers should consider the potential impact of monitoring them, whether it is in their best interest to undertake that monitoring in light of the potential harms (such as psychological stress, overwork) and potential safety considerations (which may be heightened for young workers in some cases – for example when they are being trained for the first time). Employers should also ensure that minors are providing informed consent, which may require additional explanation, or parental consent for younger workers.

Example: Monitoring young people

The following example was provided to HTI by a legal service. The employer in this instance would fail to meet fair and reasonable requirements, including this factor requiring consideration of the best interests of the child.

Minors were employed by a large fast-food chain. They were concerned that their employer had placed cameras in the change rooms. The young people understood that the cameras were placed there so that their employer could ensure that they weren't using their phone at work. Because of the cameras, the young people did not change in the change room. They were also concerned that the screens displaying the CCTV footage from the change room could be seen in the restaurant.⁴⁷

Applying the fair and reasonable factors collectively, surveillance focused on tasks or work processes for clear business purposes are more likely to be legitimate. Surveillance focused on a worker's personal life or personal characteristics is less likely to be legitimate.



Example: Location tracking

A company installs location trackers in its delivery vehicles, to optimise routes, track deliveries, and for specified work health and safety purposes – including to improve emergency responses. Managers may review data for training purposes, or when a safety incident has occurred, with input from drivers. This is all outlined in a policy provided to workers during induction, and there is a notice on the dashboard of company vehicles stating that GPS tracking is in use. Where drivers have arrangements to use the vehicle for dual work and personal uses, the driver can switch off the GPS tracker after hours.

This is likely to be legitimate. The location tracking is for legitimate, clearly defined and communicated purposes, which are linked to the worker's job description and hours, with safeguards in place to prevent purpose creep, misuse or unfairness.

Example: Call emotion analysis

A customer service company analyses call data to assess 'negative sentiment' from workers, using an AI system. Staff deemed more 'negative' by the AI are automatically downgraded against performance metrics that feed into their KPIs. It is unclear how the system makes these assessments.

This is likely to be illegitimate because it is an unnecessary and disproportionate use of surveillance. As well as being privacy intrusive, sentiment analysis tools have known accuracy problems, and can be unlawfully discriminatory. There are less intrusive ways to assess the quality of customer service calls – such as through customer surveys.

Application to high-risk technologies and contexts

Ministerial power to proscribe certain technologies

There may be a small category of surveillance tools, products and services which present an unacceptable risk to workers' human rights, and would not be acceptable for use in any workplace. In other words, some tech-enabled surveillance is not fair and reasonable in any standard workplace. Hence, the Minister should have the power to proscribe individual or classes of products and services, where they would unjustifiably limit workers' rights. To ensure a considered approach, this power should be conditioned on prior public consultation and input from regulators such as the Fair Work Ombudsman or the OAIC.

While the fair and reasonable test would remain technology neutral and flexible, such a ministerial power would account for situations where a particular technology poses an exceptionally high, unmitigated risks. If the minister exercised this power via a legislative instrument, it would allow for rapid responses to dangerous new and emerging technologies, while maintaining parliamentary oversight.

As mentioned above, smart glasses may fall into this category. Workplace use cases include workers being required to wear smart glasses to record their activities for a manager to observe; or managers wearing smart glasses themselves to covertly surveil workers. Smart glasses also pose new harassment risks for women in the workplace.⁴⁸ The high level of risk associated with smart glasses, combined with little identifiable workplace benefits, may prompt the use of this ministerial power.

Emotion recognition technology may also meet this threshold, because it is highly privacy intrusive, and due to its accuracy and discrimination problems. The European Union has banned emotion recognition technology for use in workplace contexts for these reasons.⁴⁹

Application to high-risk government operational contexts

In certain government contexts, such as in policing, corrections and national security, a bespoke approach to worker monitoring may be appropriate. In these high-risk operational contexts, there are heightened impacts on human rights of members of the public, such as the right to life, and a unique public accountability justification for the adoption of certain forms of monitoring. For example, a number of Australian police forces have legislation that provides for officers wearing and operating body-worn cameras. Nonetheless, it is still important that the use of worker monitoring for public safety and accountability purposes does not creep into unnecessary surveillance of workers for other purposes, such as to monitor general performance.

There is some targeted or bespoke regulation and numerous operational instruments that apply to the use of body-worn devices at the state and territory levels.⁵⁰ Police, corrections and national security bodies are overseen by dedicated oversight bodies, such as police integrity commissions and federal, state and territory Ombudsmen.⁵¹ Dedicated regulation of these devices in high-risk operational contexts is appropriate due to the particular balance of rights that are necessarily engaged (both for officers, and the public at large). Directly applying the Fair Work Act criteria to these contexts would also involve some complexity, as the employment rights for many of these professionals (such as state and territory police officers) occur at the state and territory level, with only partial coverage by the Fair Work Act.

For these reasons, it is preferable to further develop targeted regulation for worker monitoring in these operational contexts. In the medium term, consideration should be given to developing a dedicated approval process for police, corrections and other security bodies' use of worker monitoring tools, taking into account any existing bespoke regulations, and the application of fair and reasonable principles to their specific operational contexts.

Appendix B

Concurrency

As noted above, the intention is for the ‘fair and reasonable’ requirements in the Fair Work Act to apply concurrently with existing state and territory laws that regulate some other aspects of worker surveillance, both directly and indirectly.

To this end, there should be an express preservation of state and territory surveillance laws in the drafting of the ‘fair and reasonable’ provisions in the Fair Work Act. This can be drafted using similar language to ss 106D and 112 of the Fair Work Act, which preserve the operation of state and territory laws in respect of leave and entitlements.

The amendments to the Fair Work Act should be expressed as incremental, minimum obligations that apply in addition to any requirements under state and territory laws. Provision should also clarify that they are not an authorisation of surveillance (including where surveillance is otherwise prohibited under state or territory laws). It may also be prudent to clarify that the fair and reasonable requirement is not applicable when a covert surveillance warrant is granted under state and territory laws.

Simplification of state and territory laws

To enable simplification and consistency, the federal government should coordinate with states and territories to update existing laws that regulate worker surveillance at the state and territory level.

NSW and the ACT are the only two jurisdictions that have dedicated workplace surveillance laws. Other states indirectly regulate worker surveillance through ‘surveillance devices’ legislation and/or general state privacy laws, and there is a lack of certainty regarding how these general acts apply in the workplace, as well as significant gaps in coverage. This is a longstanding problem – the Australian Law Reform Commission recommended that workplace surveillance laws should be made uniform throughout Australia back in 2014.⁵²

One pathway for reform would be to develop a consistent model clause applicable to worker monitoring that can be adopted in each relevant state or territory act. This clause could, for example:

- Update outdated definitions. Worker monitoring could be defined by reference to the new Fair Work Act provisions, and the existing definition of ‘worker’ in section 12 of the Fair Work Act. This would make clear that regardless of the nature of the ‘device’ used, the collection and use of personal data about workers for monitoring purposes may engage the relevant state or territory law. This will enable a consistent approach with the federal level, which adopts a technology-neutral standard.
- Adopt a single standard for notice, consent and disclosures, when an employer adopts a product or service to monitor workers, as conditions of lawfulness. For simplicity, this could involve adopting the highest standard at the state level, which currently is the *Workplace Privacy Act 2011* (ACT).
- Adopt a single set of prohibitions and bans – for example, states have inconsistent approaches to prohibitions on covert surveillance (i.e. in the absence of consent), and some states prohibit monitoring in sensitive areas such as toilets and changerooms, while others do not. Again, the most privacy-protective approach should be adopted.
- Clarify that worker-specific state and territory provisions apply to the exclusion of other general state and territory provisions related to surveillance or surveillance devices.

Endnotes

1. Adapted from several academic sources that draw on the same base definition by David Lyon, *The Surveillance Society: Monitoring Everyday Life* (Simon and Schuster, 2001). See also Henry Parkes, *Watching me, watching you: worker surveillance in the UK after the pandemic* (Institute for Public Policy Research, March 2023) 7 <<https://www.ippr.org/articles/worker-surveillance-after-the-pandemic>>.
- 2.. See, e.g., Irene Tung et al, *When Bossware Manages Workers: A policy agenda to stop digital surveillance and automated decision-system abuses* (National Employment Law Project, July 2025) 4 <<https://www.nelp.org/insights-research/when-bossware-manages-workers-digital-surveillance-automated-decision-system-abuses/>>.
- 3.. Joe Atkinson and Joseph Evans, *Negotiating the future of work: legislating to protect workers from surveillance* (Institute for Public Policy Research, May 2025) 7 <<https://www.ippr.org/articles/negotiating-the-future-of-work-surveillance>>.
- 4.. Troy Henderson, Tom Swann and Jim Stanford, *Under the employer's eye: Electronic monitoring & surveillance in Australian workplaces* (Centre for Future Work at the Australia Institute, November 2018) 5 <<https://futurework.org.au/report/under-the-employers-eye-electronic-monitoring-surveillance-in-australian-workplaces/>>.
5. See, e.g., Troy Henderson, Tom Swann and Jim Stanford, *Under the Employer's Eye: Electronic monitoring & Surveillance in Australian Workplaces* (Centre for Future Work at the Australia Institute, November 2018) 18 <<https://futurework.org.au/report/under-the-employers-eye-electronic-monitoring-surveillance-in-australian-workplaces/>>; Danielle E Thompson, 'Tracking Apps Monitor Remote Employees' Performance: And Invade their Privacy', *The Conversation* (online, 8 June 2025) <<https://theconversation.com/tracking-apps-monitor-remote-employees-performance-and-invade-their-privacy-256261>>; Victorian Trades Hall Council, Submission No 28 to Legislative Assembly Economy and Infrastructure Committee, Parliament of Victoria, *Inquiry into Workplace Surveillance* (31 July 2024) 9 <https://www.parliament.vic.gov.au/496277/contentassets/8a1ba32158e7487ca24163f168e5a2a1/submission-documents/submission-028---vthc---31072024_redacted.pdf>; Katie Miller, 'Are you being Watched while Working? What Hybrid Workers Need to Know', *University of New South Wales* (Blog Post, 18 September 2023) <<https://www.unsw.edu.au/newsroom/news/2023/09/are-you-being-watched-while-working--what-hybrid-workers-need-to>>; Alysa Blackham, 'Setting the Framework for Accountability for Algorithmic Discrimination at Work' (2023) 47(1) *Melbourne University Law Review* 63, 97, 109; Annette Bernhardt, Lisa Kresge, and Reem Suleiman, *Data and Algorithms at Work: The Case for Worker Technology Rights* (UC Berkeley Labor Center, November 2021) 15–16 <<https://laborcenter.berkeley.edu/data-algorithms-at-work/>>.
6. Kirstie Ball, *Electronic monitoring and surveillance in the workplace: literature review and policy recommendations* (European Commission, 2021) 7–8 <<https://op.europa.eu/en/publication-detail/-/publication/e7e6f646-4694-11ec-89db-01aa75ed71a1/language-en>>; Henry Parkes, *Watching me, watching you: worker surveillance in the UK after the pandemic* (Institute for Public Policy Research, March 2023) 17 <<https://www.ippr.org/articles/worker-surveillance-after-the-pandemic>>; Amy Vatcha, 'Workplace surveillance outside the workplace: an analysis of e-monitoring remote employees', *iSChannel* (2020) 15(1) 4–9; Chase Thiel et al, 'Monitoring employees makes them more likely to break rules', *Harvard Business Review* (online, June 2022) <<https://hbr.org/2022/06/monitoring-employees-makes-them-more-likely-to-break-rules>>.
7. 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>>.
8. 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>>.
9. 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>>.
10. David Marin-Guzman, 'CBA Faces Fight over "Big Brother" Staff Tracking', *Australian Financial Review* (online, 6 August 2026) <<https://www.afr.com/work-and-careers/workplace/cba-faces-union-fight-over-big-brother-staff-tracking-20260806-p60lut>>.
11. 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>>.
12. Kyle Orland, 'Report: Meta Will Train AI Agents by Tracking Employees' Mouse, Keyboard Use', *Ars Technica* (online, 22 April 2026) <<https://arstechnica.com/ai/2026/04/meta-will-use-employee-tracking-software-to-help-train-ai-agents-report/>>.
13. See, e.g., Anthony Cuthbertson, 'Workers Are Training AI and Robots to Replace Them. It Could End Badly', *Independent* (online, 5 May 2026) <<https://www.independent.co.uk/tech/ai-job-replacement-robots-meta-b2967096.html>>.

14. Legislative Assembly Economy and Infrastructure Committee, Parliament of Victoria, *Inquiry into Workplace Surveillance* (Final Report, May 2025) 53 <<https://www.parliament.vic.gov.au/get-involved/inquiries/inquiryintoworkplacesurveillance/reports/>>.
15. Case study provided to HTI by a legal service, during project consultations (edited).
16. Victorian Trades Hall Council, Submission No 26 to House of Representatives Standing Committee on Employment, Education and Training, Parliament of Australia, *Inquiry into the Digital Transformation of Workplaces* (2024) 7–8 <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Employment_Education_and_Training/DigitalTransformation/Submissions>.
17. 'The Future of Work Report 2021: Data Explorer', *Herbert Smith Freehills Kramer* (Web Page) <<https://insights.hsfkramer.com/fow2/p/9>>.
18. Minderoo Foundation and Talbot Mills polling (March 2026) [Note, these materials have not been published elsewhere].
19. 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>>.
20. Zoe Jay Hawkins and Johanna Weaver, *Earning Trust: Unlocking AI Adoption for Australians* (Policy Spotlight Report, May 2026) 1 <<https://techpolicy.au/earning-trust/>>.
21. Minderoo Foundation and Talbot Mills polling (March 2026) and qualitative research (July 2026).
22. 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/>>.
23. Attorney-General's Department (Cth), *Privacy Act Review* (Final Report, 2022) 116–20 <<https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report>>.
24. See *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1, art 6(1)(f).
25. Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth) 5.
26. See, e.g., Michelle Rowland, 'Albanese Government Raises Privacy Concerns over "Smart Glasses"' (Media Release, 7 August 2026) <<https://ministers.ag.gov.au/media-centre/albanese-government-raises-privacy-concerns-over-smart-glasses-07-08-2026>>.
27. The Fair Work Act imports the definition of 'worker' from s 7(1) of the *Work Health and Safety Act 2011* (Cth).
28. 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>.
29. *Fair Work Act 2009* (Cth) ss 351, 365, 527F, 576(1)(h), (la); *Australian Human Rights Commission Act 1986* (Cth) ss 3(1), 11(1)(a)–(aa), 46P; *Sex Discrimination Act 1984* (Cth) s 28B; 'Discrimination', *Fair Work Commission* (Web Page) <<https://www.fwc.gov.au/workplace-disputes/other-workplace-disputes/discrimination>>; 'Consumer Data Right Regulatory Action Policy', *Office of the Australian Information Commissioner* (Web Page, June 2020) <<https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/consumer-data-right-regulatory-action-policy>>; 'MOU with the Australian Competition and Consumer Commission: Consumer Data Right' *Office of the Australian Information Commissioner* <<https://www.oaic.gov.au/about-the-OAIC/our-corporate-information/memorandums-of-understanding/current-memorandums-of-understanding/consumer-data-right/mou-with-the-australian-competition-and-consumer-commission-consumer-data-right>>
30. Attorney-General's Department (Cth), *Privacy Act Review* (Final Report, 2022) 69–70 <<https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report>>.
31. 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>>.
32. Australian Labor Party, *Delivering Real Change: Australian Labor Party Draft National Platform* (July 2026) 29–30 <https://laborconference.org.au/files/2026_ALP_Draft_National_Platform.pdf>.
33. 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>>.

34. *Inter-Governmental Agreement for a National Workplace Relations System for the Private Sector* (2009) <<https://www.dewr.gov.au/download/16994/inter-governmental-agreement-national-workplace-relations-system-private-sector-2009/40084/inter-governmental-agreement-national-workplace-relations-system-private-sector-2009/pdf>>.
35. 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/>>.
36. Attorney-General's Department (Cth), *Privacy Act Review* (Final Report, 2022) 120 <<https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report>>
37. Attorney-General's Department (Cth), *Exposure Draft Privacy Amendment (Personal Data Protection) Bill 2026* (August 2026) 12-13 <<https://consultations.ag.gov.au/rights-and-protections/privacy-reform/>>. Note that these factors have been re-ordered into consecutive steps for the purposes of the worker-specific requirements.
38. Australian Government, Government Response: Privacy Act Review Report (September 2023) 8 <<https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF>> .
39. See Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines* (May 2026) 25 [B.117] <https://www.oaic.gov.au/___data/assets/pdf_file/0032/263777/12-May-Consolidated-APP-Guidelines-Updated-Chapter-3.pdf>.
40. See e.g., Office of the Victorian Information Commissioner, *Information Privacy Principles Guidelines: IPP 1 – Collection* (November 2019) 5–6 <<https://ovic.vic.gov.au/wp-content/uploads/2019/11/IPP-1-2019.B.pdf>>.
41. This aligns with a human rights proportionality-based approach. Similar principles apply in other legal contexts. For example, the 'Briginshaw standard' provides that in civil proceedings, more convincing evidence is required to establish an allegation on the balance of probabilities if the allegation is of a particularly serious nature: *Briginshaw v Briginshaw* (1938) 60 CLR 336, 361–2 (Dixon J).
42. See discussion in Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report No 123, June 2014) 100–102 <https://www.alrc.gov.au/wp-content/uploads/2019/08/final_report_123_whole_report.pdf>.
43. 'Young Workers: Overview', *Safe Work Australia* (Web Page) <<https://www.safeworkaustralia.gov.au/safety-topic/managing-health-and-safety/young-workers/overview>>.
44. See, e.g., Institute for Public Policy Research, "'Dystopian' Worker Surveillance Techniques Likely to Disproportionately Affect Young People, Says IPPR", (Media Release, 27 March 2023) <<https://www.ippr.org/media-office/dystopian-worker-surveillance-techniques-likely-to-disproportionately-affect-young-people-says-ippr>>.
45. *Privacy and Other Legislation Amendment Act 2024* (Cth) s 26GC.
46. Office of the Australian Information Commissioner, *Privacy (Children's Online Privacy) Code 2026* (Exposure Draft, March 2026) <https://www.oaic.gov.au/___data/assets/pdf_file/0020/262631/Exposure-Draft-Childrens-Online-Privacy-Code.pdf>.
47. Case study provided to HTI by a legal service, during project consultations.
48. See, e.g., Olga Klimczak and Ella Miels, 'AI Wearables in the Workplace: What Employers Need to Know', *Herbert Smith Freehills Kramer* (Blog Post, 10 August 2026) <<https://www.hsfkramer.com/notes/employment/2026-posts/australia-ai-wearables-in-the-workplace-what-employers-need-to-know>>.
49. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)* [2024] OJ L 1689/1, art 5(1)(f).
50. See, e.g., *Crimes (Surveillance Devices) Body-worn Cameras Guidelines 2022* (ACT); *Surveillance Devices Act 2007* (NSW) s 50A; Queensland Corrective Services, *Body Worn Cameras: Custodial Operations Practice Directive* (2025) <<https://www.publications.qld.gov.au/ckan-publications-attachments-prod/resources/eef5baf6-bf8d-48bb-b336-e60a2e1a08d2/safety-and-security-equipment-body-worn-cameras.pdf?ETag=f5b2588a7df1b5c511c6bdedda9544df>>.
51. See, e.g., Law Enforcement Conduct Commission (NSW), *Review of NSW Police Force Body-worn Video Policy and Practice* (Report, March 2025) <<https://www.lecc.nsw.gov.au/publications/publications/review-of-nsw-police-force-body-worn-video-policy-and-practice-march-2025.pdf>>.
52. Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report no 123, July 2014) Recommendation 14(6) <<https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/recommendations-17/>>.

For more information

Human Technology Institute
hti@uts.edu.au

University of Technology Sydney
PO Box 123
Broadway NSW 2007

uts.edu.au