Human Technology
Institute

Surveillance Creep

Technology-enabled worker surveillance

Snapshot Report | March 2026

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.

HTI's project on technology-enabled worker surveillance

HTI is conducting a project on technology-enabled worker surveillance, with the aim of developing a law reform proposal that protects the human rights of workers. This snapshot report outlines how technology is increasingly being used to monitor and surveil workers. It highlights pressing legal and policy issues in this area, and it provides background information to support stakeholders to consider the need for reform regarding tech-enabled worker surveillance.

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

HTI expresses particular thanks to Gilbert + Tobin, which contributed expert legal research for this Snapshot Report under the leadership of the firm's partner, Simon Burns. Any errors in this Snapshot Report remain the responsibility of HTI.

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

This Snapshot Report focuses on technology-enabled monitoring and surveillance of workers. It explores the new products and tools being used to observe, track and assess workers – many of which are fuelled by artificial intelligence (AI). It also reflects on recent major shifts in how we work. Phenomena such as the growth in remote work and the gig economy are vital in understanding the rise of tech-enabled worker monitoring.

This Snapshot Report addresses a fundamental question: are our laws adequate to protect workers from harmful surveillance, and to give clear guidance to employers about what they can and can't do? The short answer is 'no'. Our laws are complex, ambiguous and contain important gaps in worker protections – making reform urgent and important. This Snapshot Report proposes reform to protect the human rights of workers, while clarifying how organisations can monitor their workers appropriately, without engaging in unreasonable surveillance.

Context: Surveillance creep

It is widely accepted that employers will check to see that their workers are fulfilling their obligations, just as oversight bodies and unions will check that employers are treating their staff appropriately. While the employment relationship assumes some monitoring of workers, not all such monitoring is reasonable. Our law must protect workers where their employer engages in overly-intrusive surveillance.

Increasing demand for new ways to monitor workers is partly explained by the fact that a higher proportion of people work outside traditional workplaces, and often provide their labour outside of a formal employer-employee relationship. That demand is being met by new tech-enabled monitoring tools, which are inexpensive and widely available. These tools are capable of more pervasive and intrusive surveillance: workers' homes, bodies and emotions are all capable of being observed and assessed.

Australia's Federal, Victorian and NSW Governments have recognised the need to address technology-enabled worker surveillance through law and policy.[1] Urgent action is needed to protect workers from the harms of unreasonable surveillance, and guide employers to adopt practices that meet their business needs without harming their workers.

There are numerous monitoring tools on the Australian market – ranging from email-tracking software, to sophisticated spyware and wearable neurotechnology. These tools are in use everywhere from factory floors, to retail stores, to truck fleets, to law offices. For people working from home or outside of a conventional workplace ('remote workers'), the boundaries between work and home are eroding as surveillance is used to peer into workers' private spaces and family life.

What is technology-enabled worker surveillance?

Technology-enabled worker surveillance refers to the monitoring of workers through technological tools for the purposes of managing and influencing their behaviour, and making workplace decisions.[2] This necessarily 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.[3]

Not all forms of worker monitoring are inherently harmful. This report aims to draw a clear line between reasonable monitoring of workers; and unreasonable worker surveillance, by reference to human rights law criteria.

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,[4] including regarding hours, pay, leave, task allocation, hiring, promotions, disciplinary actions and termination.

The term 'worker' is broad. 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.

Acceptable forms of monitoring

There are many legitimate purposes for an employer to monitor their workers, such as to ensure work health and safety, comply with the organisation's legal and other obligations, and improve productivity. However, not all motivations for monitoring workers are justified, and even where an employer is monitoring their workers for a reasonable purpose, this does not justify all forms of intrusive surveillance.

A balanced approach would take into account the employer's legitimate interests and obligations, and also workers' human rights. In achieving this balance, international human rights law suggests three key factors should be considered:

- the employer's purpose or aim in seeking to monitor their workers
- the likely impact of this monitoring on workers and any other affected individuals, and especially whether the monitoring is likely to restrict human rights
- whether the likely impact of the monitoring is justified, taking into account the employer's objective and whether any human rights restriction is reasonable, necessary and proportionate.

Harms from unreasonable tech-enabled worker surveillance

Workers subject to unreasonable technology-enabled surveillance face a range of harms:

- **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 (eg, women, young people, and people with a disability), and this can increase the risk of discrimination or unfairness for those groups.
- **Chilling effect on freedom expression and other rights:** knowing that one is, or might be, watched can prevent workers from joining a union, or speaking and moving freely – including outside the workplace.

Is worker surveillance the best way to achieve an employer's objectives?

Before adopting a tech-enabled monitoring tool, employers should ask whether this is the best way of achieving their aim. Research indicates that unreasonable surveillance can reduce performance, drive turnover, prompt rule-breaking, and damage trust between workers and employers. Many monitoring tools are simply ineffective at measuring and improving productivity in meaningful ways – for example, a productivity metric focused on how frequently a worker takes bathroom breaks provides little insight into the productivity of the worker, nor the quality of their work.

Australian laws are failing both workers and employers

Worker surveillance is regulated through a complex, confusing and gap-ridden patchwork of laws. 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.

These laws haven't kept pace with the rise of AI and related technologies, or new working arrangements since the pandemic. Monitoring tends to be justified by a worker having 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.

In relying on fictitious consent, our laws do not set clear boundaries or 'red lines' that would prohibit unreasonable surveillance. Not only does this leave workers vulnerable, employers often don't know what they can and can't do.

The way forward

Reform is urgently needed for employers and workers alike.

The Australian Government has committed to introducing a new requirement in the *Privacy Act 1988* (Cth) for organisations to act fairly and reasonably when handling personal information. This would require organisations to follow some minimum standards when collecting and using personal information, regardless of whether the individual appears to have given consent to the handling of their personal information. As explained later in this Snapshot Report, this proposed reform would better protect individuals' human rights.

HTI supports this reform commitment. HTI's preliminary view is that the law governing worker surveillance could build on this new provision, by spelling out what is 'fair and reasonable' in the specific context of worker monitoring, especially taking into account the use of AI and other new technologies. Ideally, a consistent or harmonised legal standard would apply throughout Australia, giving regulatory certainty for businesses and clarity of protection for workers. That is likely to require amendments to a small number of federal, state and territory laws.

HTI will test this preliminary view through further research and stakeholder consultation. HTI welcomes input from union, industry, civil society and government representatives.

Surveillance creep

Increased worker monitoring with the rise of new technologies

Since the beginning of work itself, employers have monitored workers to ensure that they are working to time and on task. This is to be expected: employers have a right to know whether their workers are meeting their job requirements.

Yet with the rise of AI and other technology-enabled tools, monitoring of workers has become more widespread and it covers a greater array of aspects of workers' professional and personal lives. The risk, therefore, that legitimate monitoring slides into intrusive and unreasonable surveillance is greater than it has ever been.

Three developments are driving this profound change. The first is the ready availability of a new generation of monitoring tools. Unlike human supervision, which is time and resource intensive, these new tools are relatively cost effective and accessible for Australian employers. The second is the changing nature of work since the COVID-19 pandemic. The growth in remote work and flexible working arrangements has prompted employers to look for new ways to monitor workers outside of the physical workplace, driving demand, investment in and adoption of monitoring tools. Third, emerging AI capabilities are expanding the scale and intensity of surveillance, and opening up new frontiers for monitoring – including in workers' homes, bodies, and emotions.

What new risks do AI-powered monitoring tools pose?

Reduced transparency: due to increased reliance on 'black box' AI, and seamless integration of AI tools into existing ICT systems.

Person-based monitoring: increased focus on workers' personal characteristics, in addition to their work activities.

Algorithmic management: workers are increasingly interacting with 'robot bosses' and subject to rigid automated decisions, rather than engaging with human supervisors.

Mass collection of personal data: new capabilities enable continuous data collection and aggregation from a range of sources.

Third party access: data and insights from tech-enabled monitoring tools can be used for purposes unrelated to legitimate worker monitoring.

What are some opportunities that AI-powered monitoring tools offer?

Enhanced physical safety protections: for example, for use in mines to track the location of miners and flag environmental safety hazards.

Improved cyber security: for example, secure identity verification processes for accessing confidential information on online work systems.

Productivity and planning: for example, data analysis to anticipate busy periods for resourcing, staffing and scheduling purposes.

Uptake and adoption of monitoring tools

The adoption of technology-enabled tools, and consequently the amount of worker surveillance, has risen dramatically in recent years. However, this issue is understudied in Australia. Existing data is drawn from research with different audiences, sample sizes and recency.

In Australia and internationally, the COVID-19 pandemic saw an explosion in demand for surveillance technologies.[5] Globally, the worker monitoring software market reached US$1.98 billion in size in 2024, and is projected to grow to US$6.11 billion by 2033.[6]

Polling conducted with Australian employers shows significant uptake of surveillance tools. In 2021, research undertaken by Herbert Smith Freehills Kramer found that 91 percent of surveyed Australian employers monitored their remote workers' locations through software.[7] A 2020 survey conducted by Capterra with 1400 Australian professionals found that 59 percent of surveyed business leaders used software tools to monitor their employees.[8]

However, workers themselves have low awareness of the true extent of worker surveillance – even when they are themselves subject to surveillance. A 2026 poll, commissioned by the Minderoo Foundation, found that only 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.[9]

A number of Australian unions have also conducted their own research on the prevalence of worker surveillance in a range of sectors:

- A 2025 survey by the Finance Sector Union found that 50 percent of over 1000 finance workers surveyed reported high or very high levels of workplace surveillance, with more than half reporting a negative impact on them and their work.[10]
- A 2024 survey of Victorian members of the National Tertiary Education Union found that 53 percent of 455 respondents reported worker surveillance, with the most common means being visual recording, monitoring of computer and internet use, monitoring of emails, and monitoring of worker metrics.[11]
- A 2024 survey of Victorian Trade Hall Council members found that 61 percent of respondents were aware of surveillance in their workplace, 81 percent said that the surveillance had not been discussed with them, and only one percent were given a chance to opt out.[12]

Tech-enabled monitoring tools are adopted by employers for a range of purposes. The Australia Institute's Centre for Future Work found that a central motivation of employers is to enhance their knowledge and control regarding their workers' activities when they are on the job – and, in some cases, when they are not.[13] Other common motivations in adopting worker monitoring in Australia and internationally include: optimising productivity and efficiency; disciplining workers; improving worker conduct and performance; protecting work, health and safety; complying with legal obligations; protecting work property or proprietary information; training workers; and for cybersecurity purposes.[14] Monitoring data is also used for secondary purposes such as training AI models owned by technology companies or employers.[15]

Workers’ attitudes towards monitoring practices

Recent polling, commissioned by the Minderoo Foundation, found that workers’ acceptance of tech-enabled surveillance depends on factors such as the purpose of the monitoring, the nature of the tool relied upon, and the transparency and necessity of monitoring activities.

Notably, 75 percent of surveyed workers agree that monitoring should *only* be used where it is clearly communicated and strictly necessary to check that they are meeting their job requirements. When given a binary choice between two options, a majority (52 percent) said tech-enabled surveillance and monitoring of workers is a fundamental breach of trust and privacy, compared with 38 percent who said employers are within their rights to monitor performance.

Workers are more likely to find monitoring acceptable for purposes such as protecting company property (69 percent), promoting work health and safety (68 percent), or for training purposes (65 percent). However, they are less likely to accept monitoring to track productivity (44 percent), or to observe and manage worker behaviour (39 percent).

Workers are also highly concerned about intrusive *means* of worker surveillance, such as audio surveillance (72 percent), live-screen monitoring (71 percent), location tracking (71 percent), and emotion recognition (70 percent). They are least concerned about monitoring for the purpose of automating timesheets (48 percent).[16]

Emerging monitoring tools and uses

Many technology-enabled monitoring tools are available on the Australian market. These tools are being used across a range of work contexts – from factory floors, to retail stores, to truck fleets, to law offices – to monitor workers with various roles, and levels of autonomy.

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

Home front: Surveillance software for remote work

Increasingly, tech tools are being used to monitor workers outside of conventional workplaces, when they are working from home or remotely. Work-issued and BYO devices can be transformed into surveillance devices by employers – often without workers' knowledge or genuine consent.

Example: Safetrac

In August 2025, it was reported that Safetrac, a Victorian compliance training company, installed surveillance software onto the company-issued laptops of workers who were working from home. This enabled supervisors to monitor workers' screens, and to activate microphones to record workers' audio, without the knowledge or consent of affected workers.[17] The recordings, made over two months for up to ten hours per day, picked up any sound close to the laptop. The software was capable of capturing private conversations within families, and confidential information discussed with clients.[18]

The software used by Safetrac is called Teramind. Teramind is a US-based company – one of a number of companies offering tools with similar capabilities on the Australian market.[19] An investigation by the UK not-for-profit organisation Big Brother Watch found that, where Teramind is installed on a computer, the software can track almost all activity on the computer – 'every click and keystroke'. Employers are able see a live view of their workers' screens, and the Teramind dashboard can give supervisors granular, instant, updates on staff members. A worker detected accessing job listing websites can trigger a 'behaviour alert', as can emails assessed by the software as having 'angry' sentiment.[20]

Other common forms of remote worker monitoring in Australia include tracking of email content and web activity,[21] as well as monitoring enabled by software such as Microsoft Teams – which has opt-in features like usage analytics and a location-awareness tool, and integrates data drawn from other Microsoft products.[22]

Many jobs are now performed partly or wholly remotely: from traditional 'office' or professional work, to call centre and platform work. That said, a high proportion of people working remotely are contractors or 'gig workers', who do not have formal employment relationships with the organisations for whom they work. Those people also have fewer protections as compared with formal workers, regarding the allocation of work and other workplace rights, and less negotiating power.[23]

Hearts, minds and bodies

Many technology-enabled monitoring tools collect workers' biometric and other personal information, which is then used to draw inferences about the workers' performance as well as their emotional or physical state. They include facial and speech recognition software that assess facial expressions and tone of voice to infer emotion; wearables such as headsets or chest straps that track heart rates and other physical indicators of stress and fatigue; and tools that claim to detect 'negative sentiment' in written texts or emails.[24] Emerging tools claim capabilities such as determining when workers are paying attention. For example, Fujitsu has developed an AI model that purports to assess how much a person is concentrating when performing tasks, based on their facial expressions.[25] These tools can be used in conventional workplaces and remote work contexts.

Human emotions are complex and individual, and cannot be reliably identified or classed through the use of emotion-recognition tools.[26] The ways such tools collect and categorise personal data can be unreliable, and inferences drawn from this data about workers may appear 'scientific', but are often inaccurate or impossible to verify. For example, an AI system may infer that a person's vocal tone is 'warm' or 'angry', without a clear reason for why that inference was reached. Due to a combination of unrepresentative or biased training data, and assumptions built into the design of these tools, the inferences drawn are often even less reliable for certain demographic cohorts, such as minority ethnic groups and people with disability.[27] In one documented case, an emotion recognition system assessed black faces as angrier than white faces, even when both were smiling.[28]

In addition to their propensity for error and discrimination, emotion recognition tools deeply intrude on the privacy of workers by relying on persistent surveillance to identify private feelings. Even if these tools were one hundred percent accurate, requiring workers to be subject to, for example, continuous use of facial recognition technology over the course of a work day, would be an unjustifiable interference with privacy.

Nonetheless, these tools are being relied upon to surveil workers and make workplace decisions. Recruitment is frequently cited as an example of a workplace activity where emotion analysis is used to assess prospective workers.[29] They are also being used to evaluate job engagement, attitudes and social interaction or conflict at work.

Example: Sentiment analysis

A representative from the Australian Finance Sector Union told a parliamentary inquiry that one of its members had been adversely impacted by an AI recording tool. When speaking in a recorded conversation, the member remarked 'unfortunately it's been really rainy lately', which prompted the AI to suggest the conversation had a negative sentiment.[30]

Productivity and efficiency tools

Some tools use data collected about workers' online activity, location, movement or task-completion rate to assess productivity and make AI-informed decisions or recommendations.[31] These tools assess productivity against pre-set performance metrics, which can influence pay, scheduling, or disciplinary actions. Workers may receive automated alerts, warnings or nudges to influence their behaviour, and supervisors may be provided with continuous information about how individual workers are performing, including in comparison to other workers.

There are well-documented instances of biases and inaccuracies with such AI tools.[32] Many productivity assessment tools are unreliable. A common problem is that they adopt metrics that are demonstrably useful in assessing productivity in relation to very specific work tasks (eg, fruit picking), but are much less relevant when applied to other work contexts (eg, customer service). Many of these tools measure quantity over quality of work, and do not sufficiently take into account the context in which workers operate (eg, how an influx of customers, or weather conditions, may impact productivity), nor how individual workers may differ in their work habits and style, including due to factors such as their cultural background, gender or disability.[33]

Example: Woolworths

Workers at Woolworths were monitored under a program known as 'the Framework'. Warehouse workers wore headsets which told them what items to pick, with these instructions generated using AI.[34] Each worker was then assigned a 'pick rate', which set a standard for how quickly the worker should be picking and moving items in the warehouse. This program was designed to speed up work based on algorithmic estimations of the time a worker should take to perform tasks.[35] Some criticised the Framework for failing to account for differences between workers, or the impact of incidents beyond a worker's control, affecting their pick rate. At the end of each workday, workers were given a performance score and faced potential disciplinary action if they failed to achieve a 100 percent pick rate.[36] Worker dissatisfaction with the Framework was a factor in more than 1500 workers going on strike in November 2024, leading to an estimated $140 million hit to profits.[37]

Don’t employers need to know what their workers are up to?

Employers should be able to monitor their workers, provided such monitoring respects workers’ human rights. International law sets out three criteria to determine whether such monitoring is justified.[38]

First, an employer must have a legitimate purpose in monitoring their workers (using technology or otherwise). While employers have reasonably broad discretion in satisfying this criterion, the fact that an individual is on ‘work time’ is not, on its own, a sufficient justification. For example, it would be legitimate to monitor a worker’s performance for the purpose of determining whether they are fulfilling their job requirements or to keep them safe, but monitoring a worker for the purpose of assessing their religion or their sexual orientation would not be legitimate.

Second, it is necessary to consider what impact, if any, the monitoring will have on workers’ human rights. Most human rights may be permissibly limited, including the right to privacy. Certain ‘absolute rights’ cannot be limited. For example, monitoring a worker to prevent them from leaving the premises could be a form of arbitrary detention – something that cannot be justified under any circumstances.

Third, where a non-absolute human right is limited, the limitation must be no greater than is reasonable, necessary and proportionate in the circumstances. For a measure to be ‘reasonable’, it must be rationally connected to the legitimate purpose. This means that employers should be capable of providing a reasonable explanation as to how the monitoring activity is likely to be effective in achieving the purpose. For example, if an employer’s purpose for adopting surveillance 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.

Determining whether a measure is ‘necessary’ involves consideration of any alternative options for achieving the employer’s purpose, which are less invasive of human rights. For example, it is unnecessary for employers to audio-record employees to determine whether they are completing their allocated tasks, as there are less privacy-intrusive measures available, like human or technology-enabled review of their task outputs on a given day.

Any limitation on human rights must not be disproportionate to the employer’s purpose. This involves considering several factors, including the likelihood and severity of the impact on workers’ human rights; whether there are safeguards in place to mitigate this impact (eg, opportunities for employees to provide input and challenge AI-informed decisions); and whether some affected groups are particularly at-risk or may experience disproportionate impacts (eg, neurodiverse employees may be at-risk of misclassification by emotion-recognition tools trained on neurotypical cohorts).

How does unreasonable surveillance affect Australian workers?

Unreasonable surveillance can lead to a range of harms to workers individually and to the broader Australian workforce. Gaps in existing laws exacerbate these harms. As outlined in the next section, many of the more intrusive forms of tech-enabled surveillance do not even have a clear benefit for employers – which makes their use even harder to justify.

Privacy and blurred lines between work and home life

Tech-enabled monitoring tools can provide employers access to sensitive personal information about a worker's opinions, religion, sexuality, health, finances and other information that is irrelevant to a person's job and should not factor into decisions about their work performance. Some worker surveillance practices involve a near-total loss of privacy for workers, with virtually every movement and communication tracked by their employer.[39]

Surveillance can leave workers with no private space that is 'safe' from surveillance, and untied to their job. Intimate details about workers' family lives can also be collected – for example, tools that monitor people working from home can capture information about their children.

Data collected for seemingly legitimate purposes can be used also for illegitimate purposes. This is known as 'purpose creep'. For example, cameras introduced to protect workers from abusive customers may also be used to monitor staff for behaviours that employers deem unsatisfactory. This can increase risks of data misuse and security breaches – worker data can be exposed to fraudsters, or used by third-party platforms for purposes like targeted advertising.

Accountability and access to information

Surveillance increases the power imbalance between workers and employers.[40] Workers may feel pressured to accept unwanted surveillance because they fear losing their job. Employers in turn gain access to vast amounts of information about workers, which can be used to make decisions about individual workers and alter dynamics across workforces, while workers are left in the dark about how these tools are being used on them. Workplace relations law depends on workers being able to exercise their rights and organise collectively against unfair practices. This is undermined by information asymmetries.

For example, rideshare companies such as Uber have reportedly adopted opaque AI systems that incorporate data collected on workers to determine pay for each ride – driving pay down to the lowest possible pay that workers will accept.[41] These kinds of tools create the potential for invisible systemic impacts across entire sectors.

Human dignity

Intrusive surveillance degrades the dignity of workers.[42] Ubiquitous monitoring can be experienced as *inherently* punitive and demeaning.[43] Workers who are micromanaged and constantly assessed feel a loss of autonomy and pressure to behave less like humans and more like machines. In the words of one Australian worker: 'I feel like a robot. I feel constantly monitored… I feel battered like a dog.'[44]

Work health and safety risks

Unreasonable surveillance can lead to psycho-social harms like increased stress, anxiety and other mental health risks.[45] For example, research indicates that merely being subject to emotion monitoring provokes stress.[46] One worker reported that '[surveillance is] just this constant, unnecessary, nerve-racking stress: You're trying to concentrate and in the back of your mind you know you're on camera the entire time'.[47] The Victorian Trades Hall Council reported on a use of workplace surveillance that created a 'highly dysfunctional and negative' work environment – one of the workers took their own life, and another two were placed on suicide watch.[48]

Unreasonable surveillance can also endanger physical health and safety. Productivity-maximising tools can discourage workers from taking appropriate breaks, and encourage working at an unsustainable pace. Such work intensification can increase risks of workplace accidents and physical injuries associated with repetitive strain or prolonged stasis.[49] This can also put the general public at risk: for example, transport workers pressured to meet unrealistic targets may be more prone to road accidents.[50]

Bias, discrimination and exclusion

Research shows that certain groups experience disproportionate surveillance, and are more likely to be negatively affected by technology-enabled monitoring. These groups include low-skilled workers, workers with less autonomy in the workplace, and workers with weaker bargaining positions – including young people, women, and migrant workers.[51] Women are also more likely to have flexible work arrangements, making them particularly vulnerable to surveillance in the home.[52]

When these tools are used to make work assessments or decisions, there are significant discrimination risks for legally protected groups. These include people with disability or from diverse backgrounds who look or behave outside of the 'norm' determined by an AI system's training data and design.[53] When the same tools are relied upon across organisations and sectors, discrimination can occur at scale, exacerbating existing inequalities.[54]

Chilling effects on freedom of expression and other rights

Tech-enabled surveillance can inhibit freedom of association.[55] Data analysis can be used to predict which workers may be involved in unions, and software can track whether workers write the word 'union' in their emails.[56] Some employers have used such tools to identify and penalise workers for union involvement.[57]

Even if employers are not actively using monitoring tools in this manner, knowing that one is being watched can inhibit workers from exercising their right to join a union, or to speak and move freely, including outside of work hours.[58]

Is there a business case for intrusive worker surveillance?

Surveillance tools are often promoted as boons for productivity.[59] Yet research show mixed results in practice.[60] On the contrary, there is extensive research indicating that some forms of worker surveillance, which are perceived negatively by workers, lead to a range of poor organisational outcomes.[61] Relevant factors include:

- the purpose of surveillance: workers tend to perceive a vague or unspecified purpose as excessive
- the invasiveness of the surveillance: surveillance is perceived as more invasive when it focuses on worker's thoughts, feelings, physiology, location and reputation
- transparency regarding the use of surveillance: monitoring processes that are opaque or secretive can be perceived as unfair.[62]

Such surveillance practices are linked with reduced work satisfaction and commitment to the organisation; and negative effects on workers' performance, autonomy and creativity.[63] They can also contribute to high worker turnover.[64]

Unreasonable surveillance erodes trust between employers and workers.[65] High-trust cultures are proven to support high productivity,[66] whereas fearful workers are less likely to perform at their best – in fact, excessive worker surveillance has been shown to lead to counterproductive work practices, including increasing workers' propensity for rule breaking and resistance.[67] In addition, businesses whose surveillance practices might breach existing employment or privacy law face greater reputational risks,[68] and compliance risks.[69]

Tech-enabled surveillance tools do not always do what they say on the tin, and can provide incomplete or inaccurate information to employers. For example, some tools rely on inappropriate productivity metrics that conflate 'activity' with increased productivity. Tools that measure the amount of emails a worker sent per day, the number of meetings they attended, and how active they were on their device, do not necessarily reveal anything about the quality of their work, the effectiveness of their communications, or the strength of their judgment. Such tools can also create perverse incentives to appear 'busy' rather than doing the creative thinking or collaboration required to do one's job well.[70]

There are alternatives that avoid these risks, such as outcome-focused performance management, the setting of clear expectations, and building trust across the organisation.[71]

Australian law is out of date, and out of step with the needs of workers and employers

Worker monitoring and surveillance is regulated through a range of laws at the state, territory and federal levels, including privacy law, workplace relations law, and work health and safety laws. In addition to ambiguity arising from this complexity, there are gaps that arise 'between' these frameworks.[72] The net effect is that workers are inadequately protected from surveillance-related harms, and employers face difficulties when trying to do the right thing by their business and workers.

A critical problem is that current privacy law relies on workers consenting to the use of monitoring or surveillance. As a result, many employers provide generic disclosures of surveillance in internal policies, or in employment contracts. If employers provide notice to workers of a new policy, no specific objection may be taken as consent. Once workers have accepted a contract or a policy, they generally have little understanding or control over how they are being monitored beyond that point. Due to the power imbalance between employers and workers, consent is not a fair basis for the adoption of surveillance in the workplace – in reality, workers are unlikely to raise objections if it may jeopardise their job, or a job opportunity. Consent is also undermined when intrusive surveillance goes well beyond what workers reasonably expect in the workplace.

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	? Uncertain regulation/protection
✓ Regulatory coverage/protection	⊖ Incomplete regulation/protection

The current regulatory uncertainty is bad for workers and employers

Workers are inadequately protected from surveillance-related harms. It is also difficult for workers to exercise the legal rights they do have – due to the law's uncertainty and complexity, and the significant challenge of gathering evidence about the use of these tools.

Meanwhile, employers simply don't know where they stand. This could simultaneously deter employers from monitoring workers in legitimate ways, and enable less scrupulous employers to get away with unjustified surveillance.

Due to inconsistencies between state and territory laws, protections for individual workers depend on their location. This is also a headache for businesses operating in more than one state or territory as they must comply with multiple, sometimes inconsistent, surveillance laws.[73]

Crucially, our law does not adequately reflect workers' inalienable human rights, in conventional workplaces and while working remotely. Workers should not have to accept unreasonable surveillance because they've signed an employment contract, or to trade privacy rights away because they have elected to work from home. A balanced approach is needed, and legal clarity can help employers to appropriately draw the line.

Where should we draw the line?

As outlined above, international human rights law can help us develop a balanced approach that addresses the needs of employers and the rights of workers. The three-step human rights law test provides consistent, internationally-recognised criteria to assess a broad range of surveillance practices.[74] This test has already been incorporated into domestic laws overseas.

Fair and reasonable test

The Federal Government has committed to introducing a 'fair and reasonable' test into the *Privacy Act 1988* (Cth).[75] The proposed new provision would better align the Privacy Act with international human rights law, especially by addressing the common problem that individuals often do not provide genuine, free and informed consent to the handling of their personal information. Regardless of consent, organisations would be required to meet certain minimum requirements in collecting or using an individual's personal information.

Fair and reasonable test:

In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account:

(a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances

(b) the kind, sensitivity and amount of personal information being collected, used or disclosed

(c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency

(d) the risk of unjustified adverse impact or harm

(e) whether the impact on privacy is proportionate to the benefit

(f) if the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child, and

(g) the objects of the Act.[76]

Worker surveillance is regulated by state and territory surveillance laws, and the Privacy Act applies concurrently at the federal level. While the new provision would apply in all contexts covered by the Privacy Act, HTI's preliminary view is that this provision could be fleshed out in greater detail for the specific context of worker monitoring and surveillance. That is, general terms like 'unjustified adverse impact or harm' could be defined for the specific worker surveillance context.

Ideally, such a provision would apply throughout Australia, giving regulatory certainty for businesses and clarity of protection for workers. Harmonised reform could take place by amending relevant federal, state and territory laws.

HTI will explore the following questions in consultation with stakeholders:

- Are the criteria for the fair and reasonable test an appropriate basis for assessing whether worker surveillance practices are legitimate?
- Should the criteria in the fair and reasonable test be fleshed out and adapted to the worker surveillance legal context?

How could a fair and reasonable provision apply to worker surveillance?

The scenarios outlined below demonstrate how a fair and reasonable provision could be applied to the worker surveillance context.

(a) Reasonable expectations of the affected worker

This involves considering whether a worker, acting reasonably in the circumstances of the particular employment arrangement, would expect the particular monitoring measures.

A reasonable person would have a higher expectation of privacy when they are in their own home, as compared to a typical workplace.[77] Similarly, workers are likely to expect employers 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. Workers are also unlikely to expect that data collected at work would be used for purposes entirely unrelated to work – like for sale to third parties for commercial use. The kind of notice and policies provided by an employer will influence what workers may reasonably expect.

(b) The kind, sensitivity and amount of personal information

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.

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

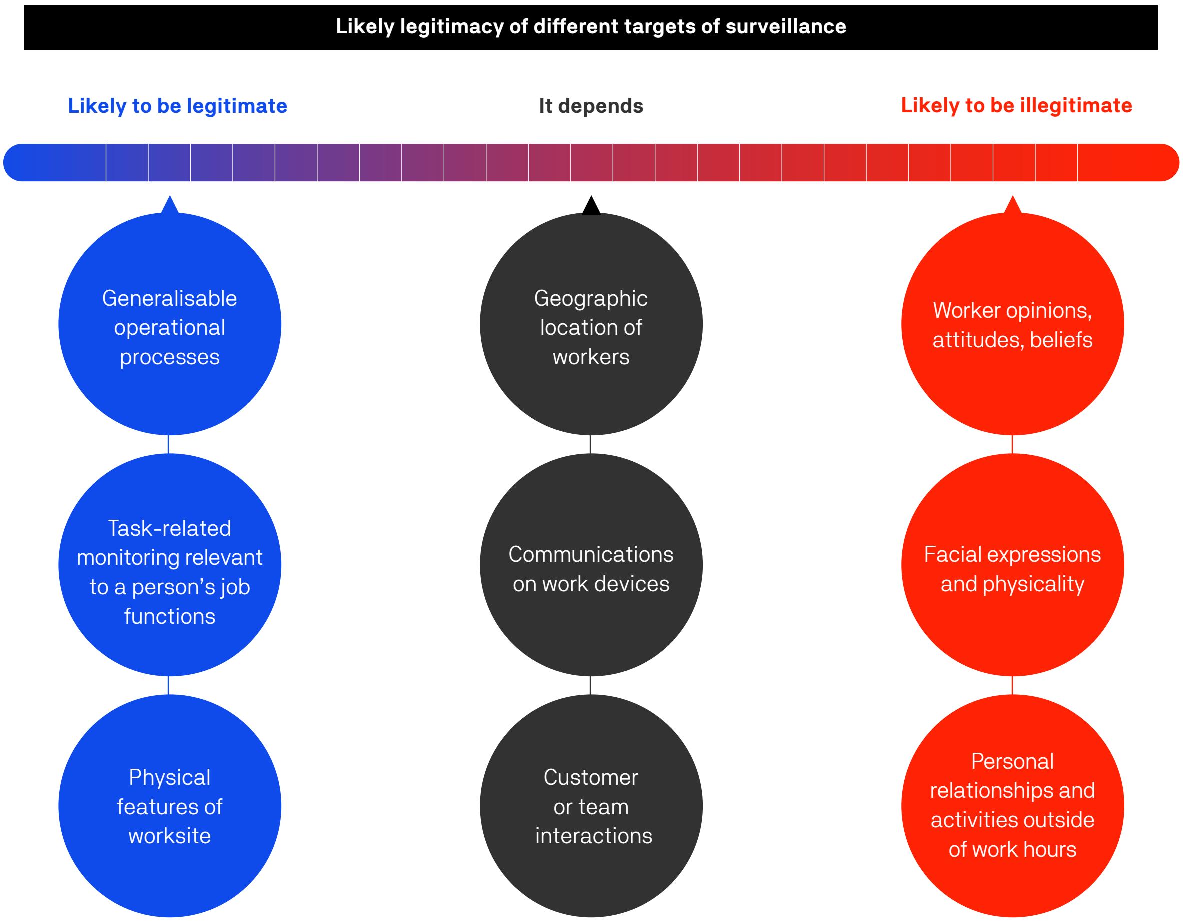
This criterion recognises that employers have a broad but finite range of legitimate purposes for monitoring workers. Meeting this criterion could involve an employer expressly setting out their purpose in conducting a monitoring activity. The monitoring would in turn need to be reasonably capable of achieving the stated purpose.

Risk of unjustified adverse impact/harm, and proportionality requirement

These related criteria reflect the human rights law proportionality test outlined above, and require the consideration of several questions:

- **What is the likelihood of adverse impact or harm to workers?** This involves consideration of what legal or human rights may be interfered with, such as privacy or worker rights protected under employment laws. It also involves assessing the severity of the possible impact on rights. 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.
- **Are there alternative options available that would be less invasive of workers' rights?** 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).
- **Are certain groups particularly at risk, or likely to experience disproportionate impacts?** For example, a productivity tool that does not take into account reasonable accommodations for people with disability will disproportionately impact that group.
- **Are there safeguards in place to mitigate potential harms?** For example, consent processes or routine audits of monitoring tools.

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


Likely legitimacy of different targets of surveillance
Likely to be legitimate
It depends
Likely to be illegitimate
Generalisable operational processes
Task-related monitoring relevant to a person's job functions
Physical features of worksite
Geographic location of workers
Communications on work devices
Customer or team interactions
Worker opinions, attitudes, beliefs
Facial expressions and physicality
Personal relationships and activities outside of work hours

Example: Use of biometrics

A clothing store introduces a new AI system that uses facial recognition to verify staff attendance. This is outlined in a new policy sent to workers, and the next day facial recognition cameras are placed at the general staff entrance of the store. When a worker objects, their manager tells them that if they refuse to comply with the system, they can look for another job.

This is likely to be an illegitimate use of surveillance. Biometrics used to identify a person involves the use of sensitive information, and requires a strong justification such as heightened or sensitive security risks, which are unlikely to apply in this example. There are alternative ways to verify physical attendance that are less intrusive, like the use of individual staff swipe cards. This example also does not involve a genuine consent process – where biometrics are adopted, employees should be provided with alternative options, without the spectre of termination or other punishment.

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 recording and analysis

A customer service company records calls that come through the company hotline for training purposes. This is clearly communicated to workers and customers.

This is likely to be a legitimate use of surveillance. Monitoring calls for training is a legitimate purpose. Workers are informed upfront, and recording is restricted to calls coming through the hotline that are directly work-related.

Another 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.

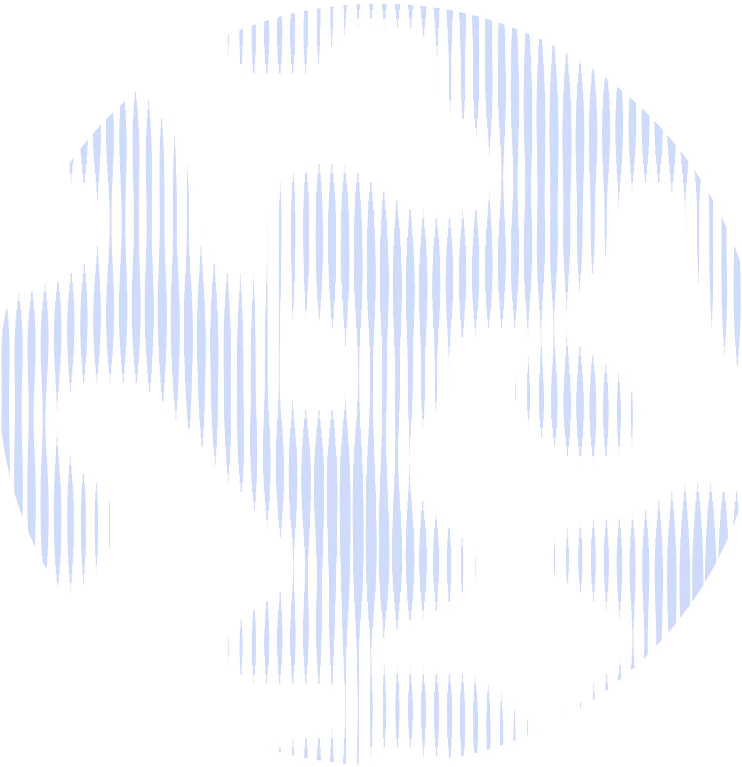
This is likely to be illegitimate because it is an unnecessary and disproportionate use of surveillance. As well as being privacy intrusive, sentiment analysis tools have known accuracy problems, and can be legally discriminatory. There are less intrusive ways to assess the quality of customer service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

Next steps

HTI is consulting with industry, union, civil society and government representatives, as well as independent experts. These consultations will focus on testing the law reform proposal set out in this Snapshot Report.

If you are interested in participating, please contact:

Sarah Sacher, Senior Responsible Technology Policy Specialist
Sarah.Sacher@uts.edu.au



Endnotes

1. See Department of Industry, Science and Resources, *National AI Plan* (December 2025) <https://www.industry.gov.au/publications/national-ai-plan>; Victorian Government, Victorian Government response 2025: 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>; Work Health and Safety Amendment (Digital Work Systems) Bill 2025.

2. 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>.

3. 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/>.

4. 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>.

5. See e.g. Jordan Turner, 'The Right Way to Monitor Your Employee Productivity', Gartner Insights (Web Page, 9 June 2022) <https://www.gartner.com/en/articles/the-right-way-to-monitor-your-employee-productivity>; Edward Segal, 'More Monitoring of Remote Workers Raises Management and Trust Issues', *Forbes* (Web Page, 25 September 2021) <https://www.forbes.com/sites/edwardsegal/2021/09/25/more-monitoring-of-remote-workers-raises-management-and-trust-issues/>; 'The Future of Work Report 2021', *Herbert Smith Freehills Kramer* (Web Page) <https://insights.hsfkramer.com/fow2/p/9>.

6. 'Employee Monitoring Software Market Research Report 2033', *Growth Market Reports* (Web Page, 2025) <Employee Monitoring Software Market Research Report 2033>.

7. 'The Future of Work Report 2021', *Herbert Smith Freehills Kramer* (Web Page) <https://insights.hsfkramer.com/fow2/p/9>.

8. Anna Hammond, '59% of Aussie SME business leaders use employee monitoring software' *Capterra* (Web Page) 10 November 2020 <https://www.capterra.com.au/blog/1799/aussie-sme-business-leaders-use-employee-monitoring-software>.

9. Forthcoming polling by Talbot Mills, commissioned by the Minderoo Foundation.

10. Finance Sector Union, *AI in the finance sector: the worker perspective* (Version 2, November 2025) 6, 12, 20 <https://www.workplaceexpress.com.au/files/2025/FSUReport.pdf>.

11. National Tertiary Education Union, Submission No 24 to Legislative Assembly Economy and Infrastructure Committee, *Inquiry into Workplace Surveillance* (30 July 2024) 7 <https://www.parliament.vic.gov.au/496273/contentassets/52a37f959d7c4724b8f8aee8d59e856e/submission-documents/submission-024---national-tertiary-education-union---30072024---redacted.pdf>.

12. Victorian Trades Hall Council, Submission No 28 to Legislative Assembly Economy and Infrastructure Committee, Parliament of Victoria, *Inquiry into Workplace Surveillance* (31 July 2024) 14, 33 <https://www.parliament.vic.gov.au/496277/contentassets/8a1ba32158e7487ca24163f168e5a2a1/submission-documents/submission-028---vthc---31072024_redacted.pdf>.

13. 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/>.

14. 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* (Web Page, 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* (Web Page, 18 September 2023) <https://www.unsw.edu.au/newsroom/news/2023/09/are-you-being-watched-while-working--what-hybrid-workers-need-to>.

15. Alyisa 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/wp-content/uploads/2021/11/Data-and-Algorithms-at-Work.pdf>; Annette Bernhardt, Lisa Kresge and Reem Suleiman, ‘The Data-Driven Workplace and the Case for Worker Technology Rights’ (2022) 76(1) *ILR Review* 3, 10 <https://journals.sagepub.com/doi/full/10.1177/00197939221131558>.

16. Forthcoming polling by Talbot Mills, commissioned by the Minderoo Foundation.

17. David Marin-Guzman, ‘Company turned laptops into covert recording devices to monitor WFH’, The Australian Financial Review (24 August 2025) <https://www.afr.com/work-and-careers/workplace/company-turned-laptops-into-covert-recording-devices-tomonitor-wfh-20250822-p5mp0z>.

18. David Marin-Guzman, ‘Company turned laptops into covert recording devices to monitor WFH’, The Australian Financial Review (24 August 2025) < https://www.afr.com/work-and-careers/workplace/company-turned-laptops-into-covert-recording-devices-tomonitor-wfh-20250822-p5mp0z>.

19. See, e.g., ‘Employee Monitoring Software’ *Capterra* (Webpage) <https://www.capterra.com.au/directory/31087/employee-monitoring/software>; Sam McCleary, ‘How do Companies Monitor Remote Employees’, *HR Coach* (Web Page, 1 September 2024) <https://www.hrcoach.com.au/post/how-do-companies-monitor-remote-employees>.

20. Big Brother Watch, *Bossware: The Dangers of High-Tech Worker Surveillance and How to Stop Them* (Report, September 2024) 28-34 <https://bigbrotherwatch.org.uk/wp-content/uploads/2024/09/BosswareWebVersion.pdf>.

21. 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/>.

22. Dev Kundaliya, ‘Microsoft Teams’ New Location-Tracking Tool will Know When You’re in the Office’, *Computing* (Web Page, 11 December 2025) <https://www.computing.co.uk/news/2025/teams-tool-will-track-work-location>; Big Brother Watch, *Bossware: Bossware: The Dangers of High-Tech Worker Surveillance and How to Stop Them* (Report, September 2024) 43 <https://bigbrotherwatch.org.uk/wp-content/uploads/2024/09/BosswareWebVersion.pdf>.

23. See e.g. Jaan Murphy, *Regulating the ‘gig’ economy as a form of employment* (Briefing Book Article, 47th Parliament) <https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/Briefing_Book/47th_Parliament/GigEconomy>.

24. See e.g. Australian Human Rights Commission, *Peace of Mind: Navigating the Ethical Frontiers of Neurotechnology and Human Rights* (Report, October 2025) 40-41 <https://humanrights.gov.au/__data/assets/pdf_file/0032/70988/2509-Neurotech-Report_FINAL_ACC-1.pdf>; Stefania Marassi, ‘The Prohibition of AI Emotion Recognition Technologies in the Workplace under the AI Act’, *Wolters Kluwer* (Blog Post, 14 April 2025) <https://legalblogs.wolterskluwer.com/global-workplace-law-and-policy/the-prohibition-of-ai-emotion-recognition-technologies-in-the-workplace-under-the-ai-act/>.

25. ‘Fujitsu Develops AI Model to Determine Concentration During Tasks Based on Facial Expression’, *Fujitsu* (Web Page, 1 March 2021) <https://www.fujitsu.com/global/about/resources/news/press-releases/2021/0301-02.html>; Henry Parkes, *Watching Me, Watching You: Worker Surveillance in the UK after the Pandemic* (Institute for Public Policy Research, March 2023) 11 <https://www.ippr.org/articles/worker-surveillance-after-the-pandemic>.

26. Natalie Sheard, ‘Tech Companies Claim AI can Recognise Emotions, but the Evidence Doesn’t Stack Up’ *The Conversation*, (Web Page, 13 December 2024) <https://theconversation.com/tech-companies-claim-ai-can-recognise-human-emotions-but-the-science-doesnt-stack-up-243591>; see also Marianna Capasso et al, ‘On the Right to Work in the Age of Artificial Intelligence: Ethical Safeguards in Algorithmic Human Resource Management’ (2024) 9(3) *Business and Human Rights Journal* 346, 354 <https://www.cambridge.org/core/journals/business-and-human-rights-journal/article/on-the-right-to-work-in-the-age-of-artificial-intelligence-ethical-safeguards-in-algorithmic-human-resource-management/48C5CC4DBEDE34EEEFC1591E89C6B1A8>.

27. See e.g., Natalie Sheard, ‘Algorithm-facilitated discrimination: a socio-legal study of the use by employers of artificial intelligence hiring systems’, *Journal of Law and Society* (2025) 52, 269-291.

28. Lauren Rhue, ‘Emotion-reading tech fails the bias test’ *The Conversation* (online) 3 January 2019 <https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404>.

29. See e.g. Natalie Sheard, ‘Employment Discrimination By Algorithm: Can Anyone Be Held Accountable?’ (2022) 45(2) *UNSW Law Journal* 617, 617-648.

30. Economy and Infrastructure Committee, Parliament of Victoria, *Inquiry into Workplace Surveillance* (Report, May 2025) 28 <https://www.parliament.vic.gov.au/49a1f1/contentassets/5232a88edcc34487aa0223bcbb2c8974/laeic-60-02-inquiry-into-workplace-surveillance2.pdf>.

[31] See e.g. Merve Hickok and Nestor Maslej, ‘A Policy Primer and Roadmap on AI Worker Surveillance and Productivity Scoring Tools’ (2023) *AI and Ethics* 3, 673-687.

[32] Big Brother Watch, *Bossware: The Dangers of High-Tech Worker Surveillance and How to Stop Them* (Report, September 2024) 46 <https://bigbrotherwatch.org.uk/wp-content/uploads/2024/09/BosswareWebVersion.pdf>.

[33] Merve Hickok and Nestor Maslej, ‘A Policy Primer and Roadmap on AI Worker Surveillance and Productivity Scoring Tools’ (2023) *AI and Ethics* 3, 673-687, 680-681.

[34] Tom Barnes, ‘The Dispute Causing Empty Shelves at Woolies is a Test Case for Companies Using AI and Automation on Workers’, *The Conversation* (Web Page, 4 December 2024) <https://theconversation.com/the-dispute-causing-empty-shelves-at-woolies-is-a-test-case-for-companies-using-ai-and-automation-on-workers-245144>.

[35] Ariel Bogle, ‘”Stop All Time Wasting”: Woolworths Workers Tracked and Timed under New Efficiency Crackdown’, *The Guardian* (Web Page, 23 October 2024) <https://www.theguardian.com/business/2024/oct/23/woolworths-staff-efficiency-productivity-crackdown-timed>.

[36] Lauren Kate Kelly, ‘Why Woolworths Workers Can’t Sleep at Night: Inside the Supermarket Giant’s Controversial “Framework”’, *The New Daily* (Web Page, 24 October 2024) <https://www.thenewdaily.com.au/work/2024/10/24/woolworths-workers-framework-controversy>.

[37] Carrie LaFrenz and David Marin-Guzman, ‘Hit to Woolworths sales from strike grows to $140m, expected to rise *Australian Financial Review* (Online) 9 December 2024 <https://www.afr.com/companies/retail/hit-to-woolworths-sales-from-strike-grows-to-140m-expected-to-rise-20241209-p5kwvg>.

[38] See Parliamentary Joint Committee on Human Rights (Commonwealth), Guidance Note 1: Drafting statements of compatibility (Guidance Note, December 2014) ; UN Commission on Human Rights, Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, UN Doc E/CN.4/1985/4 (28 September 1984).

[39] See e.g. Michael Sainato, ‘”You Feel Like You’re in Prison”: Workers Claim Amazon’s Surveillance Violates Labor Law’, *The Guardian* (Web Page, 21 May 2024) <https://www.theguardian.com/us-news/article/2024/may/21/amazon-surveillance-lawsuit-union>.

[40] Henry Parkes, *Watching Me, Watching You: Worker Surveillance in the UK after the Pandemic* (Institute for Public Policy Research, March 2023) 18 <https://www.ippr.org/articles/worker-surveillance-after-the-pandemic>; Big Brother Watch, *Bossware: The Dangers of High-Tech Worker Surveillance and How to Stop Them* (Report, September 2024) 4, 19 <https://bigbrotherwatch.org.uk/wp-content/uploads/2024/09/BosswareWebVersion.pdf>.

[41] Veena Dubal, ‘On Algorithmic Wage Discrimination’ (2023) 123(7) *Columbia Law Review* 1929, 1943, 1960, 1965, 1991 <https://www.columbialawreview.org/content/on-algorithmic-wage-discrimination/>; Molly Glick, ‘Why You Might Soon Be Paid Like an Uber Driver: Even If You’re Not One’, *Slate* (Web Page, 13 October 2024) <https://slate.com/technology/2024/10/uber-lyft-gig-workers-artificial-intelligence-wage-discrimination-jobs.html>; Madeline Batt and Melodi Dinçer, ‘November 2025 Tech Litigation Roundup’, *Tech Policy Press* (Web Page, 11 December 2025) <https://www.techpolicy.press/november-2025-tech-litigation-roundup/>.

[42] See e.g. Merve Hickok and Nestor Maslej, ‘A Policy Primer and Roadmap on AI Worker Surveillance and Productivity Scoring Tools’ (2023) *AI and Ethics* 3, 673-687, 677.

[43] See Jeevan Hariharan and Hadassa Noorda, ‘Imprisoned at Work: The Impact of Employee Monitoring on Physical Privacy and Individual Liberty’ (2025) 88(2) *Modern Law Review* 333, 333-365.

[44] Victorian Trades Hall Council, Submission No 26 to Standing Committee on Employment, Education and Training, Parliament of Australia, *The Future of Work: Inquiry into the Digital Transformation of Workplaces* (2025) 27 <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Employment_Education_and_Training/DigitalTransformation/Submissions>.

[45] See e.g. Matt Scherer, Center for Democracy and Technology, *Warning: Bossware May be Hazardous to Your Health* (Report, 2021) 14-15 <https://cdt.org/wp-content/uploads/2021/07/2021-07-29-Warning-Bossware-May-Be-Hazardous-To-Your-Health-Final.pdf>; Merve Hickok and Nestor Maslej, ‘A Policy Primer and Roadmap on AI Worker Surveillance and Productivity Scoring Tools’ (2023) *AI and Ethics* 3, 673-687, 681.

[46] Kirstie Ball, *Electronic Monitoring and Surveillance in the Workplace: Literature Review and Policy Recommendations* (European Commission, 2021) 24 <https://op.europa.eu/en/publication-detail/-/publication/e7e6f646-4694-11ec-89db-01aa75ed71a1/language-en>.

[47] Danielle Abril and Drew Harwell, ‘Keystroke Tracking, Screenshots, and Facial Recognition: The Boss May Be Watching Long After the Pandemic Ends’, *Washington Post* (Web Page, 24 September 2021) <https://www.washingtonpost.com/technology/2021/09/24/remote-work-from-home-surveillance/>.

48. Standing Committee on Employment, Education and Training, Parliament of Australia, Inquiry into the Digital Transformation of Workplaces (Report, January 2025) ch 4 <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Former_Committees/Employment_Education_and_Training/DigitalTransformation/Report/Chapter_4_-_Data_privacy_and_surveillance>.

49. See e.g. Merve Hickok and Nestor Maslej, 'A Policy Primer and Roadmap on AI Worker Surveillance and Productivity Scoring Tools' (2023) *AI and Ethics* 3, 673-687, 681; Jeniffer Nahrgang et al, 'Safety at Work: A Meta-Analytic Investigation of the Link Between Job Demands, Job Resources, Burnout, Engagement, and Safety Outcomes' (2011) 96(1) *Journal of Applied Psychology* 71-94; Christine Sprigg et al, 'Work Characteristics, Musculoskeletal Disorders, and the Mediating Role of Psychological Strain: A Study of Call Center Employees' (2007) 92(5) *Journal of Applied Psychology* 1456–1466; Annette Bernhardt, Lisa Kresge, and Reem Suleiman, UC Berkeley Labor Center*, Data and Algorithms at Work: The Case for Worker Technology Rights* (Report, November 2021) 15 <https://laborcenter.berkeley.edu/wp-content/uploads/2021/11/Data-and-Algorithms-at-Work.pdf>; Thomas R Waters and Robert B Dick, 'Evidence of Health Risks Associated with Prolonged Standing at Work and Intervention Effectiveness' (2015) 40(3) *Rehabilitation Nursing* 148 <https://pmc.ncbi.nlm.nih.gov/articles/PMC4591921/>.

50. Evidence to the Select Committee on Adopting Artificial Intelligence, Australian Senate, 21 May 2024 (Jack Boutros, Transport Workers Union of Australia) <https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commsen/27986/&sid=0005>.

51. See e.g., Henry Parkes, *Watching me, watching you: worker surveillance in the UK after the pandemic* (Institute for Public Policy Research, March 2023) 20 <https://www.ippr.org/articles/worker-surveillance-after-the-pandemic>; Parliament of Victoria*, Inquiry into workplace surveillance* (May 2025) 61 <https://www.parliament.vic.gov.au/inquiryintoworkplacesurveillance>.

52. See e.g. Australian Bureau of Statistics (ABS), *Household Impacts of Covid-19 Survey* (February 2021) <https://www.abs.gov.au/statistics/people/people-and-communities/household-impacts-covid-19-survey/feb-2021>; Working Women Queensland, *Working under the lens: Protecting worker's rights with AI-powered workplace surveillance on the rise* (November 2025) <https://brq.org.au/wp-content/uploads/2025/10/WWQ-AI-Project-Report-Workplace-surveillance-2025.pdf>.

53. Merve Hickok and Nestor Maslej, 'A policy primer and roadmap on AI worker surveillance and productivity scoring tools' (2023) *AI and Ethics* 3, 673-687, 680.

54. Merve Hickok and Nestor Maslej, 'A policy primer and roadmap on AI worker surveillance and productivity scoring tools' (2023) *AI and Ethics* 3, 673-687, 679; See also Natalie Sheard, 'Employment discrimination by algorithm: Can anyone be held accountable?' *UNSW Law Journal* (2022) 45(2) 617-648.

55. See e.g. David Marin-Guzman, 'Glencore ordered to stop "quasi-militaristic" surveillance of CFMEU members' *Australian Financial Review* (Online) 24 October 2017 <https:// www.afr.com/policy/economy/glencore-ordered-to-stop-quasimilitaristic-surveillance-of-cfmeu-members-20171024-gz6vwe>.

56. Steven Greenhouse, '"Constantly monitored": the pushback against AI surveillance at work' *The Guardian* (Online) 7 January 2024 <https://www.theguardian.com/technology/2024/jan/07/artificial-intelligence-surveillance-workers> ; Annette Bernhardt, Lisa Kresge, and Reem Suleiman, *Data and algorithms at work: The case for worker technology rights* (UC Berkeley Labor Center, November 2021) 16 <https://laborcenter.berkeley.edu/wp-content/uploads/2021/11/Data-and-Algorithms-at-Work.pdf>.

57. Annette Bernhardt, Lisa Kresge, and Reem Suleiman, *Data and algorithms at work: The case for worker technology rights* (UC Berkeley Labor Center, November 2021) 16 <https://laborcenter.berkeley.edu/wp-content/uploads/2021/11/Data-and-Algorithms-at-Work.pdf>; Josh Taylor, 'Amazon denies it planned to spy on workers in Sydney to stop them unionising' *The Guardian* (Online) 4 September 2020 <https://www.theguardian.com/technology/2020/sep/04/amazon-appears-to-be-trying-to-prevent-sydney-workers-from-unionising-using-workplace-data>.

58. Merve Hickok and Nestor Maslej, 'A policy primer and roadmap on AI worker surveillance and productivity scoring tools' (2023) *AI and Ethics* 3, 673-687, 678.

59. See e.g. 'Employee Productivity Monitoring' *KickIdler* (Webpage) <https://www.kickidler.com/features/productivity-analysis.html>.

60. Elisa Giasoca et al, 'Stress-inducing or performance-enhancing? Safety measure or cause of mistrust? The paradox of digital surveillance in the workplace' *Journal of Innovation & Knowledge* (2023) 8(2) <https://www.sciencedirect.com/science/article/pii/S2444569X23000537?via%3Dihub>; Melissa Wheeler, 'Does tracking your employees actually make them more productive? *The Conversation* 25 October 2024 < https://theconversation.com/does-tracking-your-employees-actually-make-them-more-productive-242027>.

61. 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>.

62. 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.

63. 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>.

64. VMWare, *The virtual floorplan: New rules for a new era of work* (2021) <https://blogs.vmware.com/emea-en/2021/12/new-vmware-research-how-to-find-the-balance-between-spying-and-performance-measurement-in-the-new-world-of-hybrid-working>; Kirstie Ball, *Electronic monitoring and surveillance in the workplace: literature review and policy recommendations* (European Commission, 2021) 7 <https://op.europa.eu/en/publication-detail/-/publication/e7e6f646-4694-11ec-89db-01aa75ed71a1/language-en>.

65. Kirstie Ball, *Electronic monitoring and surveillance in the workplace: literature review and policy recommendations* (European Commission, 2021) 7 <https://op.europa.eu/en/publication-detail/-/publication/e7e6f646-4694-11ec-89db-01aa75ed71a1/language-en>; Merve Hickok and Nestor Maslej, 'A policy primer and roadmap on AI worker surveillance and productivity scoring tools' (2023) *AI and Ethics* 3, 673-687, 681.

66. See e.g., Paul Zak, 'The Neuroscience of Trust' *Harvard Business Review* (Online) January 2017 <https://hbr.org/2017/01/the-neuroscience-of-trust>.

67. 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>; Kirstie Ball, *Electronic monitoring and surveillance in the workplace: literature review and policy recommendations* (European Commission, 2021) 7 <https://op.europa.eu/en/publication-detail/-/publication/e7e6f646-4694-11ec-89db-01aa75ed71a1/language-en>.

68. Lucia Stein and Damien Carrick, 'Job recruitment tools could "enable discrimination" against marginalised groups, research finds' *ABC News* (online) 8 May 2025 <https://www.abc.net.au/news/2025-05-08/ai-job-recruitment-tools-could-enable-discrimination-research/105258820>.

69. As is the case with Safetrac, which is facing multiple civil claims and a criminal investigation.

70. Merve Hickok and Nestor Maslej, 'A policy primer and roadmap on AI worker surveillance and productivity scoring tools' (2023) *AI and Ethics* 3, 673-687, 681.

71. Karlie Cremin, 'Why monitoring remote workers crosses the line and destroys workplace culture' *HR Leader* 26 September 2025 <https://www.hrleader.com.au/business/27333-why-monitoring-remote-workers-crosses-the-line-and-destroys-workplace-culture>.

72. Parliament of Australia, House of Representatives Standing Committee on Employment, Education and Training, *The Future of Work: Inquiry into the Digital Transformation of Workplaces* (January 2025) 47 <https://parlinfo.aph.gov.au/parlInfo/download/committees/reportrep/RB000516/toc_pdf/TheFutureofWork.pdf>.

73. Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123, July 2014) 276, [14.9] <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/14-surveillance-devices/>.

74. See Parliamentary Joint Committee on Human Rights (Commonwealth), Guidance Note 1: Drafting statements of compatibility (Guidance Note, December 2014); UN Commission on Human Rights, Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, UN Doc E/CN.4/1985/4 (28 September 1984).

75. Australian Government, *Government Response: Privacy Act Review Report* (September 2023) 8 <https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report>.

76. Attorney-General's Department, *Privacy Act Review Report* (February 2023) 120 <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>.

77. See discussion in Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (ALRC Report 123, July 2014) 100-102 <https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/14-surveillance-devices/>.

Human Technology
Institute

For more information

Human Technology Institute
hti@uts.edu.au

University of Technology Sydney
PO Box 123
Broadway NSW 2007

uts.edu.au

UTS CRICOS 00099F

Stock photographs: Adobe Stock Images (www.stock.adobe.com).