**Submission No 24**

# INQUIRY INTO WORKPLACE SURVEILLANCE

**Organisation:** National Tertiary Education Union (NTEU)

**Date Received:** 30 July 2024

National Tertiary Education Union

# SUBMISSION OF THE NATIONAL TERTIARY EDUCATION UNION TO THE INQUIRY OF THE VICTORIAN LEGISLATIVE ASSEMBLY ECONOMY AND INFRASTRUCTURE COMMITTEE INTO WORKPLACE SURVEILLANCE

**Prepared by NTEU members:**
**Associate Professor Alysia Blackham, Melbourne Law School**
**Dr Jake Goldenfein, Melbourne Law School**
**Professor Joo-Cheong Tham, Melbourne Law School and NTEU Victorian Assistant Secretary (Academic Staff)**

This submission has the following sections:

A. The growing dangers of workplace surveillance
B. The Victorian tertiary education sector as a case-study in workplace surveillance
C. The absence of effective regulation of Victorian workplace surveillance
D. Workplace Privacy Principles as a framework for dedicated workplace surveillance legislation

Sections A and B address Terms of Reference (2)-(8) of the inquiry. Section C addresses Term of Reference (1) while Section D deals with Terms of Reference (9) and (11).

The submission makes three recommendations:

> *Recommendation 1:* The Office of the Victorian Information Commissioner audits Victorian universities for their compliance with the *Privacy and Data Protection Act 2018* (Vic) and be adequately resourced for this purpose.
>
> *Recommendation 2:* The Victorian Parliament enacts a statute dedicated to regulating workplace surveillance.
>
> *Recommendation 3:* The statute in Recommendation 2 be based on six Workplace Privacy Principles:
>
> **1)** Comprehensiveness
> **2)** Transparency
> **3)** Freedom of association and the centrality of trade unions
> **4)** Legitimate purpose and proportionality
> **5)** Governance and accountability
> **6)** Effective compliance and enforcement.

## A THE GROWING DANGERS OF WORKPLACE SURVEILLANCE

Surveillance is a prevalent feature of workplaces. Managers collect and analyse information about workplace operations to realise efficiencies and manage worker conduct, safety, and performance. But as the means, purposes, and scope of workplace surveillance have evolved over time, so has its capacity to cause harm, expropriate value from workers, and augment managerial power.

While surveillance is not unique to workplaces, the dangers of workplace surveillance are distinctive because of:

- *The centrality of paid work to lives and livelihood:* Paid work is typically the main source of income for workers and a central source of meaning given that most waking hours of workers are devoted to performance of such work;

- *The breadth and depth of employer power:* The ability of employers to control the performance of work is a defining feature of contracts of employment[1] as is the corresponding obligation of obedience imposed on employees.[2] Given the centrality of work to lives, this contractual power provides a broad scope to managerial prerogative. The vital importance of paid work to livelihoods also means such power is highly consequential – loss of job through dismissal can often mean severe financial insecurity;[3]

- *The imperative of counter-vailing worker power:* There are two key sources of the imbalance of power in employment relationships. First, there is, as explained above, the condition of subordination imposed by the contract of employment.[4] Second, the creation of the employment relationship itself is characteristically marked by inequality. This was recognised early on by Justice Henry Bournes Higgins, Australia's most influential industrial judge. In the *Harvester* decision which established the principle of a living wage under Australian labour law,[5] Justice Higgins justified legislative regulation on the basis that it countered 'the usual, but unequal, contest, the higgling of the market for labour, with the pressure for bread on one side, and the pressure for profits on the other'.[6] In a later decision, his Honour said that:

---

[1] See *Hollis v Vabu* (2001) 207 CLR 21.
[2] See *Adami v Maison de Luxe Ltd* (1924) 35 CLR 143.
[3] Robert Hale, 'Coercion and Distribution in a supposedly Non-Coercive State' (1923) 38(3) *Political Science Quarterly* 470.
[4] Hugh Collins, 'Market Power, Bureaucratic Power and the Contract of Employment' (1986) 15(1) *Industrial Law Journal* 1.
[5] Fair Work Australia, *Waltzing Matilda and the Sunshine Harvester Factor: The early history of the Arbitration Court, the Australian minimum wage, working hours and paid leave* (2011).
[6] *Ex parte H V McKay* (1907) 2 CAR 1, 3.

> The power of the employer to withhold bread is a much more effective weapon than the power of the employee to refuse to labour. Freedom of contract, under such circumstances, is surely misnamed; it should rather be called despotism in contract; and this Court is empowered to fix a minimum wage as a check on the despotic power.[7]

Not surprisingly, some have characterized employer power as a form of 'tyranny'.[8] The imbalance of power in employment relationships gives rise to the imperative of counter-vailing worker power. Otto Kahn-Freund, considered the founder of labour law as a scholarly discipline,[9] said that:

> the main object of labour law (is) to be a countervailing force to counteract the inequality of bargaining power which is inherent and must be inherent in the employment relationship.[10]

In this context, counter-vailing worker power takes two main forms: collective representation and bargaining through trade unions; and legislative protection. In the context of workplace surveillance, at present, neither of these countervailing forces is effectively limiting employer power.

In this context, we highlight six growing dangers associated with the increasing reach, depth, and ubiquity of workplace surveillance and the absence of constraint on employer power:

*1) The use of workplace surveillance for de-skilling and work intensification*

The use of surveillance and automation to increase efficiency results in jobs being broken down into granular tasks, and labour rearranged in ways that speed up work, while de-skilling and alienating workers. Work is further intensified through the automation of managerial processes that leverage surveillance, information asymmetry, and abusive gamified mechanisms that push workers to work faster and longer in order to access opaquely distributed work and compensation.[11]

*2) The encroachment into private aspects of workers lives*

With the rise of remote working, workplace surveillance has now entered workers' homes, producing new forms of intrusion into private spaces. Even at employer premises, there is

---

[7] *Federated Engine Drivers' and Firemen's Association of Australia v. Colonial Sugar Refining Co. Ltd* (1916) 22 CLR 103. See also Henry Bournes Higgins, *A New Province for Law & Order: being a review, by its late President for fourteen years, of the Australian Court of Conciliation and Arbitration* (1968).
[8] Elizabeth Anderson, *Private Government: How Employers Rule Our Lives (and Why We Don't Talk About It)* (2017).
[9] Ruth Dukes, *The Labour Constitution: The Enduring Idea of Labour Law* (2017).
[10] Quoted in Paul Davies and Mark Freedland, *Kahn-Freund's Labour and the Law* (1983) 18.
[11] Veena Dubal, 'On Algorithmic Wage Discrimination' (2023) 123 *Columbia Law Review* 1929.

increased capacity to surveill aspects of work that were previously considered 'private' (e.g. workplace conversations, taking of toilet breaks, and measuring periods of 'time off task').

*3) The amplification of work, health and safety risks*

When surveillance is used to intensify work, it increases health and safety risks. For example, in workplaces that use automated systems to measure the time taken for work tasks and evaluate worker performance against those measurements, workers take more risks and cut corners to achieve performance targets. This produces poorer safety outcomes.[12] Surveillance also creates psycho-social risks for workers due to the psychological impacts of being watched (including at workers' home), and being forced to make their activities more legible to digital surveillance systems.

*4) The discriminatory impact of workplace surveillance*[13]

There is evidence that certain groups are disproportionately impacted by workplace monitoring and surveillance: how we perceive workplace surveillance is gendered,[14] and may differ on the basis of grounds, too. It is likely that those who are over-exposed to discrimination and harassment at work are also those who are more likely to be affected by workplace surveillance. Workplace surveillance is therefore an equality issue.

*5) The monetisation of workplace surveillance data*

Data streams about the conduct of work as well as work outputs themselves are increasingly valuable as datasets for AI model training and benchmarking. As a new frontier of value creation in the digital economy, AI industries are enabling new ways for employers to expropriate value from workers. This changes the nature of the bargain in relation to workplace intellectual property, and shifts knowledge work into a type of data farming for employers to exploit through data trading.

*6) Enhanced employer control through lack of transparency and accountability*[15]

---

[12] Strategic Organizing Center, *Primed for Pain: Amazon's Epidemic of Workplace Injuries* (May 2021), available <https://thesoc.org/amazon-primed-for-pain/>; *Storeworkers - Davids Distribution Pty Limited NSW Distribution Centres Award* [1998] NSWIR Comm 597; *Metcash Trading Limited v Gheorghe Scripcariu* [2006] NSCSCA 78 (11 April 2006); Karen Gregory, '"My Life Is More Valuable Than This": Understanding Risk among On-Demand Food Couriers in Edinburgh' (2021) 35(2) *Work, Employment and Society* 316 ('"My Life Is More Valuable Than This"').

[13] Material in this section is adapted from Alysia Blackham, 'The Future of Work in an Ageing World: Priorities for Advancing Age Equality at Work' (2024) 49(2) *Alternative Law Journal* 97.

[14] Luke Stark, Amanda Stanhaus and Denise L Anthony, '"I Don't Want Someone to Watch Me While I'm Working": Gendered Views of Facial Recognition Technology in Workplace Surveillance' (2020) 71(9) *Journal of the Association for Information Science and Technology* 1074.

[15] Some material in this section is adapted from Alysia Blackham, 'Setting the Framework for Accountability for Algorithmic Discrimination at Work' (2023) 47(1) *Melbourne University Law Review* 63.

The absence of effective regulation (see Section C) can lead to a lack of transparency around surveillance in the workplace. This lack of transparency can increase the hierarchical control and power disparities that characterise the employment relationship.[16] The possibility of continuous individualized monitoring therefore encourages work intensification,[17] and – coupled with a lack of transparency – poses what Gregory describes as an 'epistemic risk'; a lack of transparency in how work is allocated 'confounds [workers'] sense of self-employment and agency'.[18] This then increases the risks of work, 'creating conditions where workers are fundamentally unsure about the rules of work.'[19] Adams-Prassl therefore argues in the context of the gig-economy that 'the real point of rating algorithms … was to exercise employer control in myriad ways.'[20] Across all workplaces,

> management automation enables the exercise of hitherto impossibly granular control over every aspect of the working day.[21] … The algorithmic boss can hover over each worker like a modern-day Panoptes, the all-seeing watchman of Greek mythology: from vetting potential entrants and assigning tasks, to controlling how work is done and remunerated, and sanctioning unsatisfactory performance-often without any transparency or accountability.[22]

Control can be exercised directly and indirectly, through instructions and directives, but also through incentives, 'nudges' and other forms of 'soft control'.

These risks of automated processes and increased employer control are amplified in cases of insecure work and employment-at-will, particularly in scenarios where work can be terminated without a reason.[23] In Australia, this is likely to affect casual employees in particular, who have no guarantee of ongoing work. Indeed, Berg argues that technology is often used – or, rather, the human users of technology often use it – to make work more precarious, invisible, insecure and of lower quality.[24]

---

[16] Valerio De Stefano, '"Negotiating the Algorithm": Automation, Artificial Intelligence, and Labor Protection' (2019) 41(1) *Comparative Labor Law and Policy Journal* 15, 31-32. See also Alysia Blackham, '"We Are All Entrepreneurs Now": Options and New Approaches for Adapting Equality Law for the "Gig Economy"' (2018) 34(4) *International Journal of Comparative Labour Law and Industrial Relations* 413, 418.
[17] Karen Gregory, '"My Life Is More Valuable Than This": Understanding Risk among On-Demand Food Couriers in Edinburgh' (2021) 35(2) *Work, Employment and Society* 316, 326.
[18] Ibid.
[19] Ibid 327.
[20] Jeremias Adams-Prassl, 'What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work' (2019) 41(1) *Comparative Labor Law & Policy Journal* 123, 132.
[21] Ibid 134.
[22] Ibid 137.
[23] Valerio De Stefano, '"Negotiating the Algorithm": Automation, Artificial Intelligence, and Labor Protection' (2019) 41(1) *Comparative Labor Law and Policy Journal* 15, 40.
[24] Janine Berg, 'Protecting Workers in the Digital Age: Technology, Outsourcing, and the Growing Precariousness of Work Automation, Artificial Intelligence, & Labor Law' (2019) 41(1) *Comparative Labor Law & Policy Journal* 69, 70.

Workplace surveillance is being used to identify and disrupt efforts by workers to collectivise and push for better working conditions. This occurs through direct monitoring of collective worker activity through trade unions as well as indirectly through the chilling effect of workplace surveillance. Contemporary warehouse workers frequently identify workplace surveillance targeting unionisation and collectivisation efforts.[25] In fact, Australia's surveillance devices regulation emerged in response to abusive monitoring of workers engaged in protected industrial action in the 1990s.[26]

Arguably, there is *systematic arbitrariness* in these six dangers. Workplace surveillance is often not necessary for the effective performance work. There is a fundamental contradiction in workplace surveillance practices: *it is growing apace with tenuous justification*. Even worse, employers are typically not required to demonstrate the justification for their surveillance practices. These practices vividly highlight that one of the main problems of digitisation is *unaccountable power*.[27]

## B THE VICTORIAN TERTIARY EDUCATION SECTOR AS A CASE-STUDY IN WORKPLACE SURVEILLANCE

For the purpose of informing this submission, a survey was emailed to Victorian members of the NTEU with the survey open for two weeks (25 June 2024 to 9 July 2024). 455 responses were received. The survey questions are in the Appendix to this submission.

The key findings of the survey are as follows:

1) **A majority of respondents believed surveillance was being conducted at their workplace**

- 53.4% of respondents reported being surveilled at their workplace (with 34.7% unsure and 11.9% reporting no surveillance);
- The three main forms of surveillance reported were:
    - Visual recording equipment (16%);
    - Monitoring of computer and internet usage (10.5%); and
    - Monitoring of emails (5.1%).

[25] Michael Sainato, 'You feel like you're in prison': workers claim Amazon's surveillance violates labor law' *The Guardian* (21 May 2024), available https://www.theguardian.com/us-news/article/2024/may/21/amazon-surveillance-lawsuit-union.
[26] Anna Johnston and Michelle Cheng, 'Electronic workplace Surveillance, Part 1: concerns for employees and challenges for privacy advocates' (2003) *Privacy Law and Policy Reporter*.
[27] Jamie Susskind,, *The Digital Republic: On Freedom and Democracy in the 21st Century* (2022) 3.

Qualitative responses from those who reported being surveilled included:

> *Surveillance has increased steadily in recent years on campus to include: heat tracking in rooms, video cameras, number plate recognition devices at point of entry, software on devices. Little information has been provided to staff about what is being collected and for what purposes.*
>
> *The university has switched over from physical keys to RFID cards tied to mobile devices as the means for accessing buildings. . . All this data is logged ostensibly for security reasons such as preventing theft. As a side effect, managers have access to data about staff whereabouts. While policies can prevent its misuse, its very existence creates a power imbalance. Managers need only drop a hint that they have access to the data to exert influence.*
>
> *Monitoring and reporting of activities via iAuditor software. Daily entry of locations and work undertaken is expected. Metrics of the amount of work done.*
>
> *There are cameras in every teaching room but we have been told nothing about them.*
>
> *Our calls with Students are monitored and Employers can see our Work Status on Calabrio.*
>
> *Moved to new offices which have camera surveillance.*
>
> *I was highly surprised to hear that attendance on campus was being tracked via some kind of university system. We have never been consulted about this.*
>
> *Monitoring office attendance through access card data and wifi data.*
>
> *People have been checking offices to see if staff are coming onto campus.*
>
> *The move from private offices to open plan 'workspaces' has increased surveillance.*
>
> *Recording of all-of-school staff meetings, both face to face and online, has been occurring for several years. . . . The recording of meetings has appeared to have had an intimidating effect on staff. Now meetings typically are tightly controlled with little / no discussion.*

2) **A significant minority of respondents believed surveillance was being conducted when working at home**

- 34.2% of respondents reported being surveilled when working from home (with 47.5% unsure and 18.3% reporting no surveillance);
- Three main forms of surveillance reported:
    - Monitoring of computer and internet usage (12.6%);
    - Monitoring of emails (6.6%); and
    - Time and performance tracking software (3.5%).

Qualitative responses from those who reported being surveilled included:

*All work is monitored emails, computer usage, location etc.*

*The change over to online live platforms for office work files has dramatically increased the monitoring that management can do and does do.*

*MS Teams has been introduced across all employee computers. I am aware Teams provides analytics on usage and in real time shows my computer activity to my manager. I only found out about this from things managers were saying about peoples availability whilst working remotely or at a different location.*

*Microsoft Teams is the biggest surveillance tool - our team is "required" to check in via a group chat to ensure we are there and to check out.*

*We have all been asked to log onto Microsoft Teams which shows everyone, including your manager when you are online. It also shows everyone when you are inactive online as it will show how long you have been inactive. This makes me nervous as I feel like that I will be judged for the time I am away, even if it is having a stretch away from my computer or going for a toilet break. We shouldn't have to be monitored in this manner as I find it very intrusive.*

*Staff are phoned for check ins at different times during the day via Teams with video which is surveillance. Staff are asked where they are particularly if in Community (Aboriginal Community). Keystrokes are monitored but I'm not sure of this extent .*

*Monitoring of internet traffic. The IT security team also told me they were able to identify specific files on my work issued computer.*

3) **A significant minority of respondents reported specific uses of data collected by employers**

- 39% of respondents reported specific uses of data collected by employers (with 60.1% unsure);
- The main uses reported were:
    - Performance management (17.7%);
    - Disciplinary actions (including dismissals) (10.5%);
    - Task allocation and monitoring (8.9%); and
    - Monitoring union activity (2.8%).

Qualitative responses from those who reported specific uses of data included:

> *It is my understanding that discussions about staff performance are held at a management level based on information obtained from programs like Canvas. They will look at data such as how many hours we are logged into a course, what materials we download or look at and upload etc. This does not account for any works undertaken online such as researching or writing new material or recording new material prior to uploading it.*
>
> *I'm extremely unhappy that we are teaching in ways that are monitored - some of this is about monitoring students' progress but it's still not ok. We are required to use specific software to record lectures that enables their detailed analytics on student performance but also then us of course if students are not attending. . . . It is assumed by being employed by the university you consent to all your lectures being recorded and used for AI in the future, I was told. We have to record lectures which are then stored by the university to be used how they like.*
>
> *There is a lot of pressure on us academics to facilitate the recording and in some cases live-streaming of our lectures. This is problematic as it raises not only the issue of surveillance, but also the issue of intellectual property: if the University keeps a recording of our lectures (as it is doing), that content automatically becomes its intellectual property, and they are in principle free to use it in whatever way they like in the future.*
>
> *HR monitors Team chat using keywords.*

*Emails and messages via an electronic message service (Slack) have been accessed without my knowledge or consent and then used against me to try to gaslight me and to attempt to launch disciplinary action against me.*

*Emails sent to members and potential members in my work area becoming the subject of informal verbal warnings which my line managers were directed by HR (against their own will) to deliver to me.*

*My University accessed staff members e-mail and phone calls to the NTEU and Branch Committee members/Office Bearers and used them when staff took Protected Industrial Action to discipline staff.*

*My work email has been monitored and used for disciplinary action (misconduct) against me. We know from the Peter Ridd case that this happens regularly in Australian universities.*

4) **A substantial number of respondents were unsure whether workplace surveillance was being conducted and the uses of surveillance data**

- 34.7% of respondents were unsure whether surveillance was being conducted at their workplace;
- 47.5% of respondents were unsure whether surveillance was being conducted when working from home; and
- 60.1% of respondents were unsure whether data collected was being put to specific uses.

5) **An overwhelming majority of respondents were not notified or consulted by their employer as their surveillance practices**

- 81.7% of respondents reported not being notified of their employer's surveillance practices; and
- 91.4% reported not being consulted in relation to their employer's surveillance practices.

6) **An overwhelming majority of respondents were not aware of their workplace having a published policy on surveillance**

- 51.8% reported that their workplace did not have a published policy on data surveillance; and
- 43.4% were unsure whether their workplace had a published policy on data surveillance.

7) **An overwhelming majority of respondents reported not being given the option of opting out of surveillance**

- 71.2% of respondents reported not being given such an option; and
- 27.7% were unsure whether they had been given such an option.

8) **A majority of respondents reported not being aware of how to access data their employers collected on them**

- 55.8% of respondents were unsure how to access data their employers collected on them; and
- 40.8% of respondents said they could not access data their employers collected on them.

## C THE ABSENCE OF EFFECTIVE REGULATION OF VICTORIAN WORKPLACE SURVEILLANCE

Australia's legislative response to workplace surveillance typically marginalises regulation in favour of management by consultation between workers and employers. Wright and Lund, talking specifically about the computational monitoring systems called 'engineered standards', suggest this legal treatment reflects 'an increasingly sympathetic view of the employer position and a growing hostility towards continued trade union opposition'.[28] They described the Australian workplace arbitration system as often advocating for workplace rationalization and promoting "modern" management practices, in line with Australian industrial relations reform's focus on productivity enhancement. In this context, workplace surveillance has been explicitly elided by both privacy and industrial relations regulation, and instead relegated to contractual regulation and managerial prerogative.

Existing surveillance regulation is only *marginally* relevant to data collection from and about workers, including data about work performance. In Australia these include data protection (or information privacy) laws, as well as surveillance devices regulations. Australian information privacy laws explicitly exclude workplace records however, minimising data governance requirements for employers that might otherwise constrain data collection and processing.

If information privacy laws were applicable, they would at least oblige employers to inform employees about the collection of their personal data, the purpose of its collection, who can

[28] John Lund and Christopher Wright, 'State Regulation and the New Taylorism: The Case of Australian Grocery Warehousing' (2001) 56(4) *Industrial Relations* 747.

access it, and to whom it might be disclosed. They would also impose limitations on processing and use through purpose binding rules. Although these rules would not establish sufficient limits on workplace surveillance, they could afford workers some insight into the role of performance metrics, biometric recordings, psychological tests and evaluations, and various types of behavioural data collected in workplaces. More sophisticated data protection regimes, like the EU GDPR, also include rights to not be subject to automated decisions that potentially offer further, non-derogable, pathways to consultation on the implementation of technological systems.[29]

Where workplace surveillance laws have been more successful is in matters of video and audio monitoring through state-level *Surveillance Devices Acts*. Ironically, the most far-reaching of these is the NSW regime, which emerged in response to excessive surveillance of workers engaged in industrial action against Franklins for their introduction of engineered standards. During the dispute, Franklins claimed to have video evidence of strikers causing property damage, and dismissed a worker, prompting 900 others to walk out. This pushed electronic surveillance onto the union agenda, who demanded legislative intervention on the basis that no consensus could be reached that might be embedded in contractual agreements.[30]

Resulting legislation prohibited covert surveillance, creating rights for workers to be informed in advance of proposed surveillance (i.e., and given details as to method, duration etc). But these systems apply primarily to camera and sound recording, location tracking, and computer surveillance (such as web, email, and social media monitoring). Worker performance evaluation, time and motion tools (i.e. algorithmic management), or novel mechanisms for monitoring work from home, are not covered by these laws and have not been the focus of the workplace privacy reform agenda until more recently.

We elaborate below on these failures to regulate in relation to the three laws relevant to Victorian workplace surveillance:

- the *Privacy Act 1988* (Cth);
- the *Privacy and Data Protection Act 2014* (Vic); and
- the *Surveillance Devices Act 1999* (Vic).

*a*. *Privacy Act 1988* (Cth)

[29] Damian Clifford, Jake Goldenfein, Aitor Jimenez, Megan Richardson, 'A Right of Social Dialogue on Automated Decision-Making: From Workers' Right to Autonomous Right' (2023) *Technology and Regulation* 1.
[30] Julian Sempill, 'Under the Lens: Electronic Workplace Surveillance' (2001) 14 *Australian Journal of Labour Law* 1.

While large employers and federal government entities are covered by the *Privacy Act 1988* (Cth), most small organisations (with an annual turnover of AU$3 million or less) are exempt from regulation.[31] Section 7B(3) of the *Privacy Act 1988* (Cth) also contains an exemption in relation to employee records, where those records are directly related to a current or former employment relationship.[32] The Act therefore only requires large employers to gain consent for the collection of new employee data.[33] Once collected, employee data is exempt from the Act under the 'employee records' exception. Further, 'consent' to the collection of employee data has been held to be valid even if given under threat of termination or discipline for non-compliance.[34] This offers a very limited understanding of 'consent' and its limits in the employment relationship. In *Cheikho v Insurance Australia Group Services Ltd*,[35] then, an employer's use of employee monitoring software on a work computer was implicitly upheld in an unfair dismissal claim, even though the employee was reportedly 'confused' and 'shocked' when presented with the data.

Even in regulatory grey-zones – i.e. where the information monitored is not explicitly an 'employee record' that might satisfy the exemption in the *Privacy Act*, courts have legitimated employers' surveillance exercises so long as they are directed towards demonstrating a breach of expected conduct, and are not gratuitously collecting other types of sensitive information.

The employee records exemption has been the subject of a number of law reform proposals.[36] However, the persistent absence of reform reflects a political imperative of excluding workplaces from privacy regulation in Australia in order for workplace surveillance to become a matter for the industrial relations system and its normative framework that assumes its legitimacy in service of productivity. These political decisions were made during a period of deregulation of Australian labour law, with the introduction of the *Workplace Relations Act 1996* (Cth) after the end of the Accord era. Once removed from the regulatory agenda, matters of workplace surveillance soon disappeared from enterprise bargaining agreements and Awards, becoming the content of individual workplace agreements, over which prospective workers had little power or inclination to negotiate privacy matters.

[31] *Privacy Act 1988* (Cth) ss 6C(1), 6D.
[32] *Privacy Act 1988* (Cth) s 6(1), definition of 'employee record'.
[33] *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946.
[34] *Construction, Forestry, Maritime, Mining and Energy Union v BHP Coal Pty Ltd* [2022] FWC 81.
[35] [2023] FWC 1792.
[36] Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005); Australian Law Reform Commission, *For your information: Australian Privacy Law and Practice* (2008); Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (2013).

There are, however, advantages to managing workplace surveillance as a matter of industrial relations policy rather that information privacy because, even where broadly framed as in the EU, information privacy remains a limited tool for addressing surveillance at work. First, it focuses mostly on *processes*, and creating ways to identify and manage the risks of surveillance and data collection. This risk-based approach is quite different to the *substantive* approach of labour law, and the need to ensure individual rights are protected and upheld in the workplace. Second, it largely focuses on creating and protecting *individual* data protection rights, as opposed to the collective nature of much of work. The governance of workplace data needs to go beyond 'personal information' (information or opinion about an identified or reasonably identifiable individual), which is the purview of information privacy and data protection laws. Even in the European Union, then, scholars have argued there is a need for regulation tailored specifically to the workplace, rather than relying on general data protection legislation.[37]

*b. Privacy and Data Protection Act 2018* (Vic)

This Act only applies to specified Victorian public sector organisations and does not generally apply to the private sector - section 13 of the Act clearly sets out its limited coverage. This leaves a noticeable lacuna in Victoria for smaller private sector organisations, who are not covered by federal or Victorian privacy law. Further, as under federal law, the *Privacy and Data Protection Act 2018* (Vic) is primarily focused on processes – not substantive rights or outcomes – as well as 'personal information' and *individual* data protection rights.

This means that only some (public sector) Victorian workplaces are subject to obligations under the *Privacy and Data Protection Act 2018* (Vic); where the Act applies, it potentially affords workers important data subject rights such as access and correction. However, the worker and workplace data collection and processing contemplated by that Act is made permissible by consent, meaning individual workplace agreements are sufficient to enable the types of workplace surveillance described above as causing harm to workers. This is why information privacy regimes are described as normatively concerned with channelling accepted forms of surveillance power rather than imposing limits on surveillance.[38] Regulating workplace surveillance (i.e. establishing appropriate workplace data relations) needs to be considered a matter of regulating workplace conditions rather than a matter of

[37] Antonio Aloisi and Valerio De Stefano, 'Between Risk Mitigation and Labour Rights Enforcement: Assessing the Transatlantic Race to Govern AI-Driven Decision-Making through a Comparative Lens' (2023) 14(2) *European Labour Law Journal* 283.

[38] Serge Gutwirth and Paul de Hert, 'Privacy, Data Protection, and Law Enforcement: Opacity of the Individual and Transparency of Power' in E. Claus et al (eds) *Privacy and the Criminal Law* (Intersentia, 2006).

enforcing worker information privacy at the individual level.[39] This means, then, identifying illegitimate workplace surveillance practices that workers are unable to consent to.

The findings from the NTEU survey also raise questions as to proper compliance with the *Privacy and Data Protection Act 2018* (Vic) by the eight universities established under Victorian legislation. These universities are subject to the Act because they are 'a body established or appointed for a public purpose by or under an Act'.[40]

In the NTEU survey, a high proportion of respondents indicated that:

- They were not aware of the purposes for which surveillance data was being used, raising questions as to compliance with IPP 1.3(c) which requires Victorian universities to take reasonable steps to ensure their workers are aware of the purposes for which workplace information is being collected;
- They were not aware of being able to access information collected by their employers, raising questions as to compliance with IPP 1.3(b) which requires Victorian universities to take reasonable steps to ensure their workers are aware of the fact that they can gain access to their personal information and IPP 6 (Access and Correction); and
- They were not aware of a policy setting out their employer's workplace surveillance practices, raising questions as to compliance with IPP 5 (Openness) which requires Victorian universities to set out in a document clearly expressed policies on its management of personal information.

These gaps are all the more concerning for two reasons:

- Victorian universities are 'public authorities' within the meaning of section 4(1)(b) of the *Charter of Human Rights and Responsibilities 2006* (Vic) as 'an entity established by a statutory provision that has functions of a public nature' [41] and therefore, have obligations under the Charter in relation to the right to privacy and reputation;[42] and
- Systematic non-compliance with the *Fair Work Act 2009* (Cth) in the tertiary education sector has resulted in universities being a priority area for the Fair Work Ombudsman (FWO). The FWO has explained that '(o)ur priority areas focus on industries that are at significant risk or demonstrate a history of systemic non-compliance.[43]

---

[39] Dan Callaci and Jake Stein, 'From Access to Understanding: Collective Data Governance for Workers' (2023) 14(2) *European Labour Law Journal* 253.

[40] *Privacy and Data Protection Act 2018* (Vic) s 13(1)(e). See also Office of the Victorian Information Commissioner, *Examination of Victorian universities' privacy and security policies Examination under section 8C(2)(b) of the Privacy and Data Protection Act 2014 (Vic)* (2021).

[41] *McAdam v Victoria University & Ors (Anti-Discrimination)* [2010] VCAT 1429 (3 September 2010).

[42] Section 13 and 38.

[43] https://www.fairwork.gov.au/about-us/our-role-and-purpose/our-priorities

As major Victorian employers – in 2023, employing over 36,409 full time and fractional full-time staff in Victoria,[44] and thousands more casual staff[45] – there is a need for a stronger focus on data protection and privacy in universities. Ensuring compliance with existing laws is a critical first step. This demonstrates, too, the difficulties of ensuring compliance with existing privacy laws, particularly given their complex drafting and limited scope.

> ***Recommendation 1****:* The Office of the Victorian Information Commissioner audits Victorian universities for their compliance with the *Privacy and Data Protection Act 2018* (Vic) and be adequately resourced for this purpose.

c. *Surveillance Devices Act 1999* (Vic)

There are three major shortcomings of the Act:

**1) It is highly permissive of workplace surveillance**

Part 2A of the Act (Workplace Privacy) places stringent limitations on employers knowingly installing, using or maintaining optical surveillance or listening devices to observe, list to, record or monitor the activities or conversations of workers in workplace toilets, washrooms, change rooms and lactation rooms.[46]

The Act, however, otherwise leaves workplace surveillance significantly unregulated due to:

i. *The limited application of its prohibitions relating to installation, use or maintenance of listening devices and optical surveillance devices to workplace surveillance*

These prohibitions in sections 6 (listening devices) and 7 (optical surveillance devices) respectively apply when there is a 'private conversation to which the person is not a party' and 'a private activity to which the person is not a party':

- Section 6 is likely not to apply when an employer advises its employees that workplace conversations can be recorded as there is unlikely to be a 'private conversation'. For this reason, the recording of lectures, seminars and tutorials as indicated by the NTEU survey is likely not to come within the scope of section 6; and

[44] Department of Education, *2023 Staff numbers* (2024) https://www.education.gov.au/higher-education-statistics/resources/2023-staff-numbers (Table 2.5)
[45] 5390 FTE in 2022, and likely representing many times this in headcount: Department of Education, *2023 Staff numbers* (2024) https://www.education.gov.au/higher-education-statistics/resources/2023-staff-numbers (Appendix 1.3).
[46] *Surveillance Devices Act 1999* (Vic) ss 9B-9C.

- Section 7 is likely not to apply in the similar context when an employer advises its employees that workplace activities can be video-recorded or when such recording is publicly visible . It might not apply generally to employer surveillance as it could be argued that the employer is a party to the activity (even if 'private'). For these reasons, the use of CCTV revealed by the NTEU survey is likely not to come within the scope of section 7.

*ii. It only expressly regulates the installation, use and maintenance of data surveillance by law enforcement officers*

Unlike the prohibitions relating to listening devices, optical surveillance devices and tracking devices which apply to 'a person', the prohibition relating to data surveillance devices in section 9 only apply 'law enforcement officers' under the Act – this prohibition does not apply to employers.

The data surveillance practices revealed by the NTEU survey do not come within the scope of the Act, for instance, the monitoring of:

- Computer and internet usage (including through Microsoft Teams);
- Emails; and
- Use of card swipes.

*iii. Its approach to consent fails to adequately take into account the inequalities of power in the employment relationships*

The Act fails to properly take into account the imbalance of power that characterises employment relationships [47] - particularly in relation to its approach to consent. The prohibitions in sections 6 (listening devices), 7 (optical surveillance devices) and 8 (tracking devices) are not breached if there is express or implied consent of the person being surveilled. Implied consent may be found to exist when workers continue to perform their jobs knowing that workplace surveillance is being conducted because to do otherwise would be to risk disciplinary action (including dismissal). Even express consent might prove to be a thin reed of protection if the approach taken under the *Privacy Act 1988* (Cth) is adopted with the *Surveillance Devices Act*, with 'consent' to the collection of employee data found even when given under threat of termination or discipline for non-compliance.

*iv. It fails to impose effective requirements as to legitimate purpose and proportionality*

Unlike the Australian Privacy Principles under the *Privacy Act 1988* (Cth) and the Information Privacy Principles under the *Privacy and Data Protection Act 2018* (Vic), the *Surveillance*

[47] See Section A: The Growing Dangers of Workplace Surveillance.

*Devices Act* does not impose any requirement as to legitimate purpose or proportionality. The Act, for instance, does not prohibit surveillance of union activity nor disproportionate measures such as the monitoring of the taking of toilet breaks (as reported by the NTEU survey).

**2) It fails to ensure effective transparency of workplace surveillance**

Apart from the limited situations covered by sections 6-8 where is a requirement of express or implied consent, there is no requirement to notify workers of workplace surveillance being conducted as is required under the *Workplace Surveillance Act 2005* (NSW)[48] and *Workplace Privacy Act 2011* (ACT).[49] Specifically, there is no requirement for an employer policy on workplace surveillance, let alone one that is notified to affected workers.

This laissez-faire situation is consistent with the findings of the NTEU survey that:

- An overwhelming majority of respondents were not notified by their employer as to their surveillance practices; and
- An overwhelming majority of respondents were not aware of their workplace having a published policy on surveillance.

Nor is there any requirement under the Act to notify workers of the use of surveillance data even when such use might directly affect their interests. The NTEU survey reported the secret use of surveillance data for performance appraisal and management by managers – such use is not prohibited by the Act.

**3) It fails to ensure effective accountability of workplace surveillance**

This stems from the above shortcomings (permissiveness of workplace surveillance; and lack of transparency) and also the failure of the Act to require consultation of affected workers and trade unions (as required under the *Workplace Privacy Act 2011* (ACT)).[50] The last is consistent with the finding of the NTEU survey that an overwhelming majority of respondents were not consulted by their employer in relation to their surveillance practices.

Nor does the Act provide for:

- workplace mechanisms to monitor workplace surveillance and to address collective (systemic) issues, akin to Designated Work Groups and Health and Safety Representatives under the *Occupational, Health and Safety Act 2004* (Vic);[51] or

[48] *Workplace Surveillance Act 2005* (NSW) Part 2 (Notification of workplace surveillance of employees).
[49] *Workplace Privacy Act 2011* (ACT) Part 3 (Notified Surveillance).
[50] *Workplace Privacy Act 2011* (ACT) s 14.
[51] *Occupational, Health and Safety Act 2004* (Vic) Part 7 (Representation of Employees).

- external oversight by relevant statutory agencies.

More insidiously, the Act permits surveillance that undermines accountability through trade unions and collective worker action.

## D WORKPLACE PRIVACY PRINCIPLES AS A FRAMEWORK FOR DEDICATED WORKPLACE SURVEILLANCE LEGISLATION

The growing dangers of workplace surveillance which are distinctive to employment relationships (see Section A) and the absence of effective regulation of Victorian workplace surveillance (see Section C) make a compelling case for Victorian legislation dedicated to regulating workplace surveillance.

> ***Recommendation 2:*** The Victorian Parliament enacts a statute dedicated to regulating workplace surveillance.

We submit that this legislation should be based on six Workplace Privacy Principes, namely:

1) Comprehensiveness
2) Transparency
3) Freedom of association and the centrality of trade unions
4) Legitimate purpose and proportionality
5) Governance and accountability
6) Effective compliance and enforcement.

> ***Recommendation 3:*** The statute in Recommendation 2 be based on six Workplace Privacy Principles:
>
> **1)** Comprehensiveness
> **2)** Transparency
> **3)** Freedom of association and the centrality of trade unions
> **4)** Legitimate purpose and proportionality
> **5)** Governance and accountability
> **6)** Effective compliance and enforcement.

These principles – which are elaborated below – are drawn from:

- International Labour Organisation Declarations and Conventions relevant to freedom of association and collective bargaining;

- International human rights declarations and treaties and human rights stipulated in the *Charter of Human Rights and Responsibilities 2006* (Vic);
- Privacy Principles found in the *Privacy Act 1988* (Cth) and the *Privacy and Data Protection Act 2018* (Vic) as adapted to the workplace; and
- Principles of Workers' Data Rights[52] that go beyond general privacy principles.

### *1. Comprehensiveness*

By contrast to the limited scope of the *Privacy Act 1988* (Cth), the *Surveillance Devices Act 1999* (Vic) and the *Privacy and Data Protection Act 1988* (Vic), the legislation should be comprehensive in the sense of covering:

- all workplace surveillance based on a broad definition of 'workplace surveillance' that is technologically-neutral;
- the 'workplace' understood as 'a place where work is carried out for a business or undertaking and includes any place where a worker goes, or is likely to be, while at work'[53] (to include premises where remote working occurs);
- collection, use, storage, security, disclosure and sale of workplace surveillance data and their underlying purposes; and
- worker and workplace information going beyond workers' personal information to include aggregated and anonymised worker information created through surveillance.

### *2. Transparency*

Transparency is a key aspect of the Privacy Principles found in the *Privacy Act 1988* (Cth) and the *Privacy and Data Protection Act 2018* (Vic) as well as a central principle of workers' data rights.

The legislation should be transparent in the sense of providing:

---

[52] ILO Brief on Improving Workers Data Rights (November 2022) available < https://www.ilo.org/publications/improving-workers-data-rights>; IT for Change, *Workers Data Rights in the Platformized Workplace: A new Frontier for the Labor Agenda* (June 2022) available < https://itforchange.net/workers%E2%80%99-data-rights-platformized-workplace-a-new-frontier-for-labor-agenda> ; UNI Global, *10 Principles for Workers' Data Rights and Privacy* (February 2017) available < https://uniglobalunion.org/report/principles-for-workers-data-rights/>; Dan Callaci and Jake Stein, 'From Access to Understanding: Collective Data Governance for Workers' (2023) 14(2) *European Labour Law Journal* 253.

[53] This aligns with the *Work Health and Safety Act 2011* (Cth) s 8(1).

- Transparency of the various elements covered under Principle of Comprehensiveness;
- A general prohibition against covert surveillance;
- An express requirement of notification of surveillance and its uses to affected workers and trade unions;
- An express requirement of a published workplace policy covering elements under the Principle of Comprehensiveness;
- Access for workers and their representatives – such as unions and data trusts – to information about workplace surveillance (including the rationale behind surveillance and a description of the purposes and processes of automated decision-making);
- Transparency regarding automated systems, including how they monitor, evaluate, allocate and compensate work and determine disciplinary actions (including dismissals); and
- A prohibition against the use of trade secret protections by employers to avoid transparency obligations.

*3.* ***Freedom of association and the centrality of trade unions***

Freedom of association by workers through trade unions for the promotion and protection of their interests is a human right as recognised by Article 23(1) of the Universal Declaration of Human rights; Article 8 of the International Covenant on Economic, Social and Cultural Rights; and Article 22 of the International Covenant on Civil and Political Rights. It is a key principle of the International Labour Organisation's Declaration of Philadelphia and ILO Conventions 87 (Freedom of Association and Protection of the Right to Organise Convention, 1948) and 98 (Right to Organise and Collective Bargaining Convention, 1949), both of which apply to Australia which has ratified them.

ILO Convention 98 together with the ILO Declaration on the Fundamental Principles and Rights at Work recognise that the right to collective bargaining is a key aspect of freedom of association through trade unions.[54] ILO Convention 98 imposes the following obligation on Australia:

[54] International Labour Organisation, *Declaration on the Fundamental Principles and Rights at Work 1998*, para 2(a).

> Measures appropriate to national conditions shall be taken, where necessary, to encourage and promote the full development and utilisation of machinery for voluntary negotiation between employers or employers' organisations and workers' organisations, with a view to the regulation of terms and conditions of employment by means of collective agreements.[55]

The UN Sustainable Development Goals further underline the importance of freedom of association through trade unions (including collective bargaining) as central to good governance.[56] The ILO's Declaration of Philadelphia makes clear the democratic rationale of freedom of association through trade unions through its principle that:

> the representatives of workers and employers, enjoying equal status with those of governments, join with them in free discussion and democratic decision with a view to the promotion of the common welfare.[57]

The legislation should respect freedom of association through trade unions by:

- Prohibiting the surveillance of union activity in line with ILO Conventions 87[58] and 98;[59]
- Establishing collective bargaining and trade unions as central to the governance of workplace surveillance - including in determining the legitimacy of purpose and proportionality; as well as in participatory planning of data collection and analysis practices such as surveillance impact assessments (see below on 4. Legitimate purpose and proportionality and 5. Governance and accountability);
- Conferring standing on trade unions to enforce the legislation (see below 6. Effective compliance and enforcement); and
- Enabling the establishment of collective entities such as data trusts, data unions, or other non-profit organisations, to act as fiduciaries for workers that are capable of receiving, processing, and analysing worker data on behalf of workers.

[55] International Labour Organisation, Convention No 98 (Right to Organise and Collective Bargaining Convention, 1949) Article 4.
[56] The UN Special Rapporteur has held that freedom of association (including the right to strike) is included in 'fundamental freedoms' referred to in Sustainable Development Goal 16.10: *Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association,* Item 74(b) of the provisional agenda, General Assembly, 73rd Session, A/73/279.
[57] International Labour Organisation, *Declaration of Philadelphia* (1944) para I(d).
[58] International Labour Organisation, *Convention 87 (Freedom of Association and Protection of the Right to Organise Convention)* Articles 3 and 10.
[59] International Labour Organisation, *Convention No 98 (Right to Organise and Collective Bargaining Convention, 1949)* Article 1.

4. ***Legitimate purpose and proportionality***

Under the *Australian Privacy Principles,* personal information can be solicited only where 'the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.' Sensitive personal information also requires consent unless an exception applies. Given the limited applicability of ideas of consent to the employment context, given the imbalance of power in the employment relationship, there is a need for a more exacting standard to be applied to the employment relationship specifically.

We recommend, then, that there is a need for workplace surveillance to meet two substantive tests:

- It must be reasonably necessary to pursue a legitimate purpose in the employment context; and
- It must be proportionate to achieving that legitimate purpose.

These tests of reasonably necessary, legitimate purposes, and proportionality create a fair and reasonable balance between employers' objectives (of ensuring work performance and safety) with employees' interests in privacy and freedom of association.

These tests should be oriented towards worker dignity, autonomy and welfare in the context of data-driven technologies at work, and be grounded in the recognition of the imbalance of power that defines employment relationships. As such, individual consent alone is not sufficient for meeting these tests. Worker autonomy requires collective and participatory processes (including collective bargaining where there is a union presence) – *these tests should deemed not be met unless there are such processes*.

Whether a measure is proportionate should take into account the extent to which it infringes or limits other rights and interests, including the right to privacy under the *Charter of Human Rights and Responsibilities 2006* (Vic). It should also have strong regard to the fact that workplace surveillance is typically unnecessary for the effective performance of work (see Section A: The growing dangers of workplace surveillance). Against this context, we suggest that workplace surveillance will not have met these tests – and *therefore should be prohibited* – when:

- It causes direct or indirect harm to workers, including psychological harm, work intensification or speed-up, or worker disempowerment;
- It is intended for the monetisation of worker data, particularly if for an employer's benefit; and
- Worker data is sold to third parties.

5. ***Governance and accountability***

This principle requires workplace mechanisms that effectively regulate workplace surveillance and hold employers accountable for their surveillance practices. The legislation should include the following:

- Workplace mechanisms with representation of workers that enable regular monitoring of workplace surveillance practices (such as the Designated Work Groups under the *Occupational, Health and Safety Act 2004* (Vic));
- Collective management of worker data through a worker's data trust, fiduciary, or equivalent entity that is capable of receiving, processing, and analysing worker and workplace data on behalf of workers, and empowered to exercise data rights on behalf of workers ;
- Where there are workers represented by a union, an obligation on the employer to use reasonable endeavours to address workplace surveillance matters in a collective agreement with the union;
- Provision of oversight of workplace surveillance by an independent statutory agency (including through regular audits of workplace surveillance practices); and
- Regular review of the legislation and its effectiveness.

6. ***Effective compliance and enforcement***

The questions raised by the NTEU survey as to the compliance of Victorian universities with the *Privacy and Data Protection Act 2018* (Cth) illustrate the importance of this principle which is closely associated with Principle of Governance and Accountability. In addition to the elements of this latter Principle, the legislation dedicated to Victorian workplace surveillance should provide for:

- A properly-resourced independent statutory agency with adequate powers of investigation and enforcement;
- Standing to be conferred on trade unions, individuals and groups of workers to enforce the provisions (as is the case under the *Fair Work 2009* (Cth);[60] and
- Adequate penalties, including civil and criminal penalties and denial of access to Victorian government procurement contracts under the Victorian Government's *Fair Job Code*.[61]

[60] *Fair Work Act 2009* (Cth) s 539.

[61] https://www.buyingfor.vic.gov.au/fair-jobs-code-suppliers-and-businesses

## APPENDIX: QUESTIONS IN SURVEY SENT TO VICTORIAN MEMBERS OF THE NATIONAL TERTIARY EDUCATION UNION ON WORKPLACE SURVEILLANCE

To the best of your knowledge, is surveillance being conducted at your workplace via any of the following means:

- Audio recording equipment
- Visual recording equipment (including CCTV and body cameras)
- Monitoring of computer and internet usage
- Monitoring of emails
- Location tracking devices (including GPS and Bluetooth)
- Biometric authentication
- Time tracking and performance software
- None of the above
- Unsure
- Other

To the best of your knowledge, is surveillance being conducted when you are working from home via any of the following means:

- Audio recording equipment
- Visual recording equipment (including CCTV and body cameras)
- Monitoring of computer and internet usage
- Monitoring of emails
- Location tracking devices (including GPS and Bluetooth)
- Biometric authentication
- Time and performance tracking software
- None of the above
- Unsure
- Other

To the best of your knowledge, has surveillance at your workplace increased in the past five years?

- Yes
- No
- Unknown

To the best of your knowledge, is the data collected through employer surveillance activities being used for:

- Task allocation and monitoring
- Performance management
- Disciplinary actions (including dismissals)
- Monitoring union activity

- Unsure

Has your employer notified you of its surveillance practices?
- Yes
- No
- Unknown

Has your employer consulted you in relation to its surveillance practices?
- Yes
- No
- Unknown

To the best of your knowledge, does your workplace have a published policy on data surveillance?
- Yes
- No
- Unknown

Were you given the option to opt out of surveillance?
- Yes
- No
- Unknown

Can you access the data your employer has collected on you?
- Yes
- No
- Unknown

What has been your experience of workplace surveillance? Please provide as much detail as possible about this.

Do you consent to the National Tertiary Education Union providing your response to the Victorian Parliamentary Inquiry into Workplace Surveillance?
- Yes
- No