

**Submission
No 29**

INQUIRY INTO WORKPLACE SURVEILLANCE

Organisation: Australian Services Union (ASU), Victorian and Tasmanian
Authorities and Services Branch

Date Received: 31 July 2024

About the ASU

The Australian Services Union (ASU) is one of Australia's largest unions, representing 135,000 members across diverse industries.

The union's Victorian and Tasmanian Authorities and Services Branch represents workers in local government, social and community services, energy, water, IT, transport, and public authorities.

The ASU welcomes the opportunity to make a submission to the Economy and Infrastructure Committee of the Legislative Assembly on workplace surveillance in Victoria.

Introduction

This submission discusses workplace surveillance and its encroachment on workers' rights. It details the impact on workers, including reduced trust in the workplace, reduced privacy at work, and a loss of job satisfaction. It also outlines the risk to workers of the use of the product of surveillance to discipline workers.

With the rapid advancement of technology, the methods and frequency of employers surveilling workers are ever-expanding. Workplace surveillance encompasses various forms, such as the use of cameras, audio devices, and other technologies to monitor workers' movements, productivity, adherence to workplace operations, policies and procedures as well as driving behaviour and use of vehicles and plant. Employers also use monitoring software on computers to observe screens in real-time, track click and keystroke rates, and access emails and other communications. This surveillance extends to gathering biometric data and retaining ownership or selling data. Surveillance, and particularly over-surveillance, has negative impacts on workers and workplaces.

This submission is informed by the Australian Services Union's day-to-day work representing workers across Victoria in diverse industries. More importantly, it reflects the experiences and concerns of ASU members, obtained from more than 380 responses to an online survey conducted in July 2024.

In addition to reflecting the views and workplace experience of ASU members, this submission makes recommendations on addressing the current regulatory gap concerning workplace surveillance. This regulatory gap has allowed employers to surveil workers without proper oversight, creating occupational health and safety risks for workers.

Current Practices of Workplace Privacy and Surveillance

Workplace surveillance is not new. Surveilling workers has been a feature of work for as long as one person has materially benefited from the labour of another. However, the increasing prevalence of electronic surveillance and monitoring in workplaces is having detrimental effects on workers in every occupation and in every industry.

More than ever before, workers are electronically surveilled from the moment they arrive at work, and for many, this surveillance extends beyond work to surveillance of workers in their non-work time.

“Increased surveillance of employees accompanying the move to work-from-home during the pandemic and other socio-technological developments have amplified long-standing concerns that employee tracking, electronic performance measurement and other forms of workplace surveillance are becoming both more common and more intrusive.”¹

The expansion of electronic surveillance beyond the time workers are present in the workplace is important because, as identified by the Victorian Law Reform Commission almost two decades ago, “an employer’s use of technology may not only affect privacy in the workplace but also has the potential to blur the distinction between a worker’s activities at work and his or her private life”.²

In contemporary workplaces electronic workplace surveillance and monitoring can include:

- Automated systems to collect consumer ratings and staff evaluation
- Biometrics (such as finger scans, facial recognition, retinal scans)
- Closed Circuit Television (CCTV) surveillance
- Digital badges to track location, tone of voice, frequency and content of conversation
- Digital performance and quality management in production systems
- Digital profiling and social media history compilation and screening
- Electronic time-stamp and attendance systems
- Gamification: use of game-like techniques to boost attendance and work effort
- Global Positioning System (GPS) tracking in vehicles, ID cards, etc.
- Location tracking for off-site contractors and other mobile workers
- Microchipping employees to track location and activity
- Monitoring email content
- Monitoring keystrokes
- Monitoring telephone calls
- Monitoring social media content
- Monitoring web browsing
- On-call systems operationalised through text, mobile phone, or e-mail
- Radio Frequency Identification (RFID) tracking
- Swipe cards to track attendance and location
- Time-motion data compilation to track output and activity
- Wearables (such as Fitbit or chip implants) to track activity and location

3

ASU members are among workers who experience electronic surveillance and monitoring at work. Electronic surveillance in the local government, community sector, water, energy, and transport

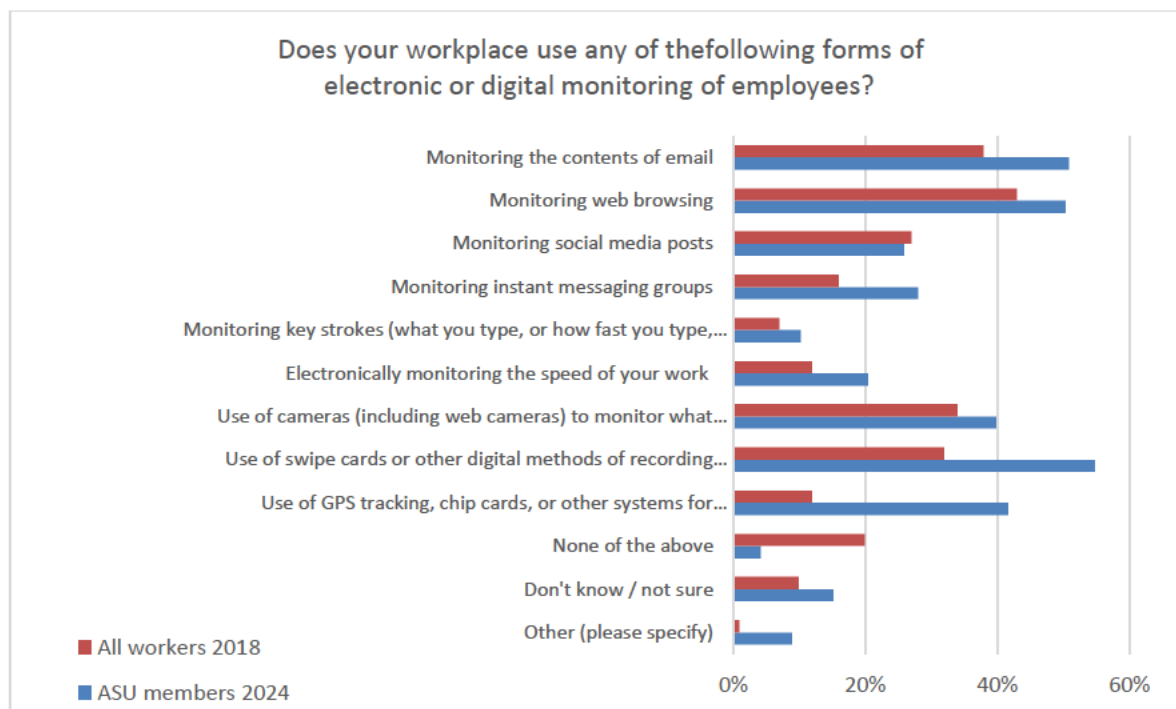
¹ Brown, M and Witzleb, N 2021, 'Big Brother at work – workplace surveillance and employee privacy in Australia', *Australian Journal of Labour Law*, vol. 34, no. 3, pp. 170-199.

² Victorian Law Reform Commission 2005, *Workplace Privacy: Final Report*, Victorian Government, p.17. Available at: <https://www.lawreform.vic.gov.au/project/workplace-privacy/>

³ Henderson, T, Swann, T, and Stanford, J 2018, *Under the Employer's Eye: Electronic Monitoring and Surveillance in Australian Workplaces*, Centre for Future Work, The Australia Institute, p.11. Available at: <https://futurework.org.au/report/under-the-employers-eye-electronic-monitoring-surveillance-in-australian-workplaces/>

sectors appears to be very high, with many workers experiencing more than one form of electronic monitoring or surveillance.

A recent survey of ASU members found they generally experience higher rates of electronic monitoring and surveillance than reported in a 2018 survey of workers across Australia.^{4 5}



High levels of surveillance and monitoring are “now common in the workplace, including automated time and task tracking, real-time monitoring of computer activities, stress and emotion detection, GPS tracking, and algorithmic systems designed to make significant decisions about employees”.⁶

Types of electronic monitoring and surveillance where ASU members are showing a much higher rate of surveillance are the use of swipe cards or other digital methods of recording attendance, monitoring the contents of email, and monitoring instant messaging groups. By far, the largest difference was in the use of GPS tracking on chip cards or other systems to monitor the location of employees.

This shows a comparatively high level of surveillance at work experienced by ASU members.

The high level of surveillance experienced by ASU members can probably be attributed to an increase in surveillance across the workforce.

If the past is any guide, employers will seek to increase the electronic monitoring and surveillance of workers using new technologies and by applying existing technologies to the task of worker surveillance.

As the level of surveillance increases, the intrusion into workers' lives will also increase, requiring a strong policy response from the Victorian Parliament to safeguard workers' safety at work, privacy

⁴ Australian Services Union 2024, ASI member survey, July.

⁵ Henderson, T, Swann, T, and Stanford, J 2018, Under the Employer's Eye: Electronic Monitoring and Surveillance in Australian Workplaces, Centre for Future Work, The Australia Institute, p.11. Available at: <https://futurework.org.au/report/under-the-employers-eye-electronic-monitoring-surveillance-in-australian-workplaces/>

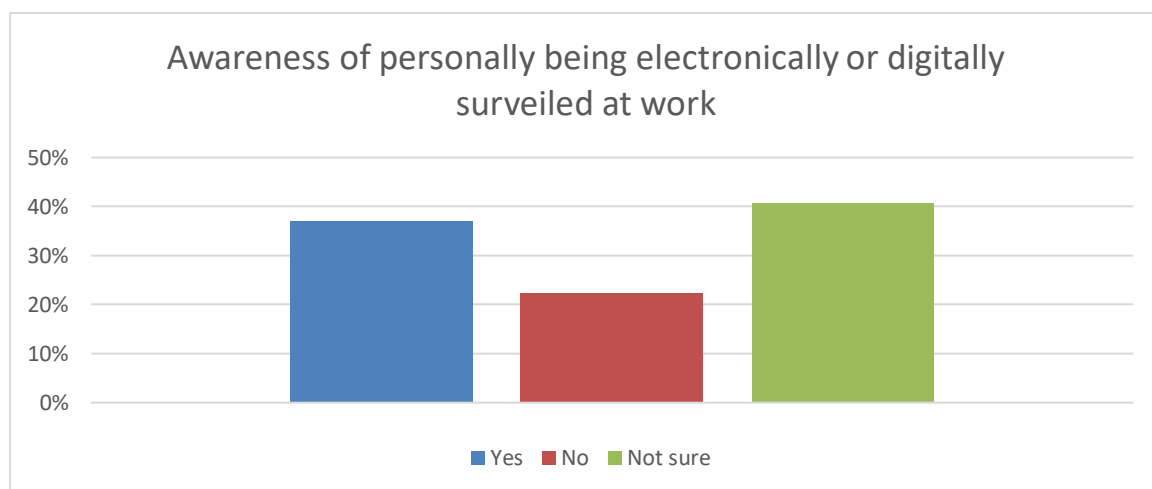
⁶ Vitak, J and Zimmer, M, 2023, Journal of Computer-Mediated Communication, Volume 28, Issue 4. Available at <<https://academic.oup.com/jcmc/article/28/4/zmad007/7210235>>

and to protect workers from the threat of arbitrary disciplinary procedures based solely on the often-poisoned fruit of electronic surveillance and monitoring.

Impact of Workplace Surveillance

The proliferation of electronic workplace surveillance and monitoring raises significant issues regarding privacy, autonomy, and the potential misuse of information. Employees often lack sufficient awareness and understanding of the extent and nature of surveillance they are subject to, which can lead to a feeling of constant oversight and stress.

While ASU members are aware of the high level of surveillance in their workplace, a disturbingly large proportion are unaware if their employer has ever used any of the forms of surveillance identified in the chart above to supervise or monitor their work or behaviour.



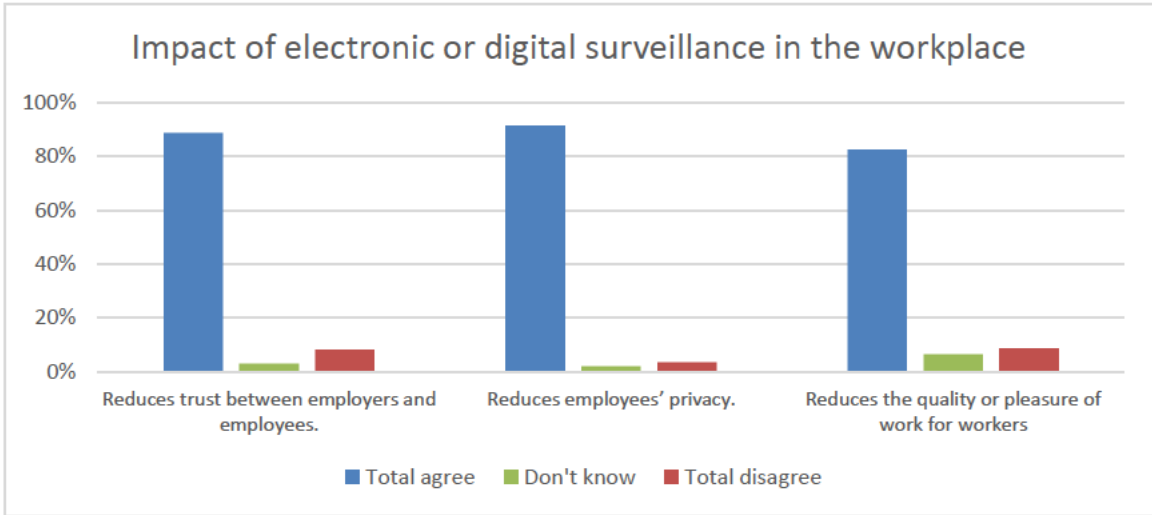
This significant proportion of ASU members who are not sure if they had been surveilled at work (40%) is concerning, indicating some employers are making little or no effort to inform workers they are the subject of electronic monitoring.

An individual worker's knowledge of whether they are being surveilled at work and the nature of any surveillance is essential to eliminating the risks to workers of workplace surveillance. This risk is compounded by the rapid pace of change around surveillance at work. Additionally, a lack of knowledge among workers makes it impossible for there to be genuine workplace consultation, affective risk assessments, and informed consent from those being surveilled.

Almost all respondents to the ASU's survey agree employers should tell employees when any form of electronic or digital surveillance is used in the workplace, with 92 per cent agreeing with this statement.

As noted earlier, the electronic monitoring and surveillance of workers is not benign. It has negative implications for workers experience at work and for their future employment opportunities.

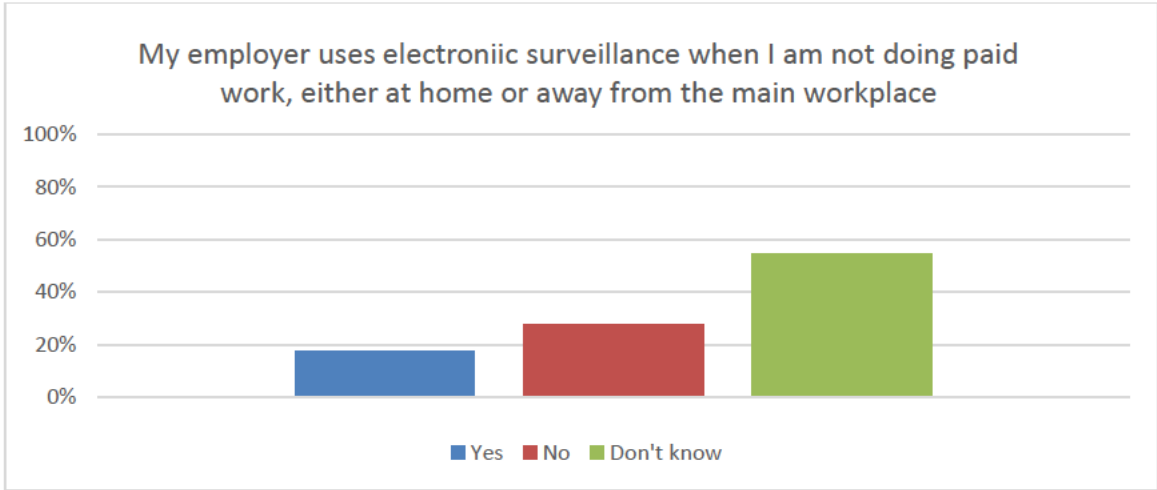
Regarding their work experience, ASU members overwhelmingly agree that electronic or digital surveillance reduces trust between employees and employers (20% agree and 68% strongly agree), reduces workers' privacy (23% agree and 61% strongly agree), and reduces the quality or pleasure of work (22% agree and 61% strongly agree).



The loss of trust, reduction in privacy and reduction in the quality or pleasure of work are not abstract concepts for many ASU members.

A local government worker observed electronic monitoring and surveillance shifts the objective of work, *“the work is transformed/evolves from working on the task to working to the measure. Preoccupation with the measure takes away from quality, autonomy and enjoyment.”* The same worker noted *“how patronising [it is] to have a toilet break timed.”* A worker in the energy industry highlighted the pervasiveness of workplace surveillance: *“everything you do in a day from minute to minutes (sic), even if you’re late two minutes from the toilet you get told off. Also, you gets (sic) told off if there’s more than one person goes (sic) to the toilet at the same time from the same team.”*

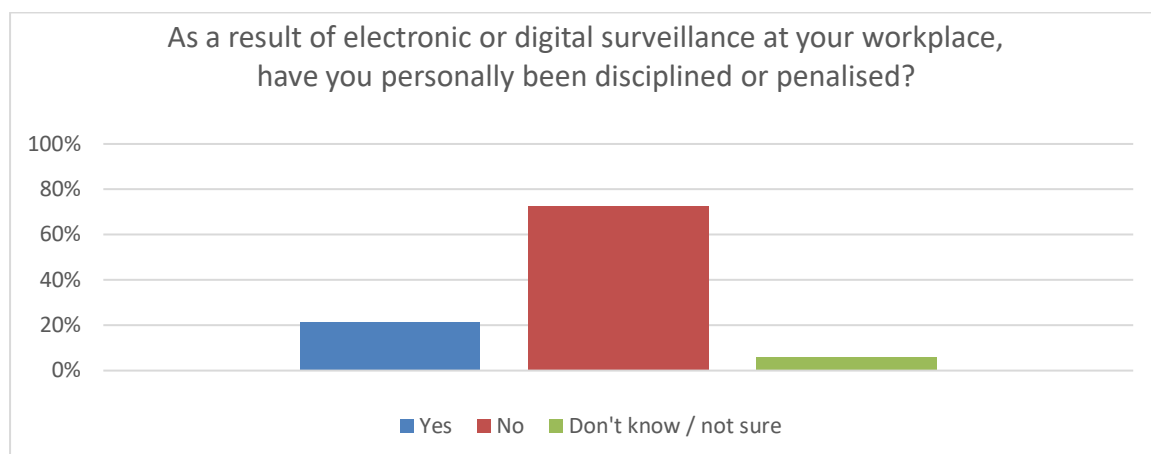
The negative effects on workers are not limited to surveillance and monitoring while on the clock or at a work location but extend into their personal lives beyond work.



18 per cent of respondents in the ASU survey report being electronically monitored when not doing work, either at home or away from their main workplace. More than half of all respondents did not know whether they were being electronically surveilled while not doing paid work.

Designed to monitor workers, electronic or digital surveillance is often used to discipline workers.

The recent survey of ASU members found a higher proportion of workers disciplined or penalised as a result of electronic surveillance than reported in a 2018 survey of workers across Australia.^{7 8}



The most common forms of discipline or penalty were being sanctioned by employer (27%) or a disciplinary letter or mention on employee’s record (13%). Workers also reported losing responsibility at work and reduced hours. A very small number of workers reported being dismissed from their jobs.

However, disciplining or penalising workers based on electronic or digital surveillance alone can be arbitrary and unfair. The recollection of one local government worker perfectly captures the risk to workers of overzealous use of surveillance for disciplining workers: *“I got questioned 1 (sic) Saturday for putting down 1600 nock (sic) off time when I got back to the yard at 3:30 but the GPS doesn’t recognise that for the last 30 mins I was Greasing and putting New Blades on the Grader.”*

Workers are not the only ones experiencing the downside of electronic surveillance and monitoring. According to respondents to the ASU survey, workplace monitoring and surveillance reduces productivity. Two per cent of respondents indicated workplace electronic or digital surveillance makes them generally more productive, 43 per cent said it made no difference to their productivity, 34 per cent said it made them generally less productive and 21 per cent did not know.

Workers who indicated workplace surveillance makes them generally less productive had insightful comments on how workplace surveillance had affected them:

A community sector worker noted, “As a team leader, the increased expectation to engage with surveillance tasks takes away from the real work I need to do, which is supporting workers in order to obtain better outcomes for our clients. I am fatigued by all of the different platforms and checks and measures now required and the benchmarks are constantly changing, which is an additional resource drain.” A local government worker said, *“I know I am being monitored. For that reason, I do only what I am required to do and nothing over and above. I no longer respect the organisation.”*

Most importantly, the safety of workers is at risk from workplace surveillance.

⁷ Australian Services Union 2024, ASI member survey, July.

⁸ Henderson, T, Swann, T, and Stanford, J 2018, Under the Employer’s Eye: Electronic Monitoring and Surveillance in Australian Workplaces, Centre for Future Work, The Australia Institute, p.11. Available at: <https://futurework.org.au/report/under-the-employers-eye-electronic-monitoring-surveillance-in-australian-workplaces/>

Responses from ASU members to an open-ended survey question asking how workplace surveillance affected them make disturbing reading and highlight the need for specific protections for workers' occupational health and safety.

"Anxiety and nightmares related to work for being monitored and disciplined for unfair reasons." Local government worker.

"Reduced trust with employer and adds stress to my already stressful job." Community sector worker.

"Pressure to be on time regardless of traffic, roadworks, school and breakdowns. No quality time with clients. Too much pressure." Local government worker.

"Contributes to low morale and motivation and decreases my psychological safety in the workplace." Community sector worker.

"Significant workplace stress as I constantly feel watched even in my own personal space." Local government worker.

"I was stressed and anxious. Anytime I looked away from the screen or wasn't typing or clicking, I was worried I was being monitored and performance managed." Local government worker.

"Impact on mental health" Community sector worker.

"It used to make me very anxious. Now I couldn't care. I am counting the days down until I can leave at [council name redacted] council." Local government worker.

"Created a level of anxiety and affected my mental health & well-being." Local government worker.

"Conscious and cautious of it which impacts my mental health." Water industry worker.

"My mental health was broken (& still recovering almost a year later), I lost my income and very nearly my home." Community sector worker.

"Loss of confidence, feel being micromanaged, depressed, time off work, not productive." State authority worker.

"Mental health - feeling guilty if not working eg: having a break or making a coffee etc if you are taking too long." Local government worker.

"It undermines us as professionals and makes me feel anxious and depressed." Community sector worker.

"I feel anxious, I don't take breaks. I'm afraid of being told off over small things or minor mistakes." Local government worker.

"I am also less likely to take the breaks I need in case someone notices and feels I am taking 'too long'." Community sector worker.

"Creates distrust of employer; creates anxiety/ stress for employee which affects productivity." Transport worker.

"Anxiety stress and fear." Community sector worker.

Not all ASU members are concerned with workplace surveillance. Some frontline workers feel workplace surveillance provides a benefit of increased safety. However, the overwhelming majority of workers are very concerned with the effect of surveillance on their workplace and themselves.

Regulating Workplace Surveillance

With the rapid expansion of electronic surveillance in workplaces and its already negative effects on workers, it is essential that the Victorian Parliament acts to provide greater regulation that protects workers.

The regulatory approach should be twofold. Firstly, a principle-based design is needed to ensure that developing technologies such as artificial intelligence do not outpace the regulation of workplace surveillance. And secondly, specific obligations on employers who use electronic and digital surveillance and codified preclusions on the use of electronic and digital workplace surveillance.

The European Union's General Data Protection Regulation has informed privacy standards around the world. While these protections are not a perfect fit for regulating workplace surveillance, they provide a very useful starting point for developing principles appropriate to the task.

The regulations contain seven key principles and six explicit rights.

These principles are:

Lawfulness, Fairness, and Transparency: Data must be processed lawfully, fairly, and in a transparent manner. Organisations must have a legal basis for processing personal data, such as consent, contractual necessity, or legitimate interests.

Purpose Limitation: Data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Data Minimization: Only the data that is necessary for the specified purpose should be collected and processed.

Accuracy: Personal data must be accurate and, where necessary, kept up to date. Inaccurate data should be corrected or deleted without delay.

Storage Limitation: Data should be kept in a form that permits identification of individuals for no longer than is necessary for the purposes for which the data is processed.

Integrity and Confidentiality: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

Accountability: Organizations are responsible for, and must be able to demonstrate compliance with, all these principles.

The explicit rights are:

The Right to Access: Individuals have the right to obtain confirmation as to whether their personal data is being processed and, if so, access to the data and information about the processing.

The Right to Rectification: Individuals can request correction of inaccurate or incomplete data.

The Right to Erasure ("Right to be Forgotten"): Individuals can request the deletion of their personal data under certain circumstances.

The Right to Restrict Processing: Individuals can request the restriction of processing under certain conditions.

The Right to Data Portability: Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format and to transmit it to another controller.

The Right to Object: Individuals can object to the processing of their data based on legitimate interests, public interest, or direct marketing.

While these principles and rights are clearly designed around the collection, creation, and use of personal data and not the collection and use of data gathered through workplace surveillance, they include themes relevant to regulating the use of data gathered through workplace surveillance.

However, to ensure the protection of workers, prohibitions on the use of workplace surveillance and specific obligations on employers must also be considered.

Recommendations

The ASU recommends introducing new privacy legislation that sets minimum standards for workers' rights and employers' obligations. The legislation should be broad enough to maintain relevance to workers and employers as technology develops.

The ASU supports recommendations put forward by Victorian Trades Hall Council and puts forward the following based on those recommendations:

1. Legislate new workplace privacy protections in the form of a Privacy in Working Life Act.
2. Protect workers from adverse actions based on surveillance-collected information including potential disciplinary action.
3. Ban surveillance in non-work-related areas.
4. Ban surveillance of workers outside of working hours.
5. Limit workplace surveillance to ensuring the security and safety of the premises and limit access to data to critical personnel only, with stringent confidentiality requirements..
6. Strengthen regulations governing how workers' sensitive personal data is handled.
7. Implement new psychosocial OHS regulations which recognise surveillance-related harms.
8. Engage with unions to develop a WorkSafe guide for the use and risks of workplace surveillance.
9. Ensure workers can opt-out of surveillance that threatens their health and safety.
10. A ban on covert surveillance unless authorised by a magistrate or police warrant.
11. A ban on the undisclosed resale of workers' personal data.
12. Mandatory notice, disclosure and consultation requirements for introducing or expanding surveillance in the workplace.
13. Ensure workers can access and use data collected about them at work.
14. Legislate fines for employers who violate workplace privacy legislation.
15. Ensure civil remedies are available for workers who have suffered abusive monitoring practices or mishandling of their personal data.
16. Extend powers of investigation to Unions and the Wage Inspectorate over workplace privacy violations.

In regard to the recommended Privacy in Working Life Act, the ASU also supports detailed recommendations put forward by Victorian Trades Hall Council:

1. The new PIWLA should prohibit surveillance in the workplace by employers. The prohibition must apply to optical, audio, location tracking, data surveillance, and biometrics scans.
2. A specific, non-negotiable obligation prohibiting surveillance in toilet facilities, changing rooms, staff facilities, and in lunchrooms designated for the personal use of workers.
3. Surveillance may be permissible only when it is used to ensure the safety of workers and others in the premises, to protect property, or to supervise processes.
4. Under a new PIWLA, if employers want to use surveillance they must:
 - a. Be able to demonstrate the need to protect people or property,
 - b. Give 14 days written notice to workers outlining exactly how, when, and where surveillance is to be conducted,
 - c. Meaningfully consult with workers and their union before implementing surveillance,
 - d. Take steps to ensure the safety of data storage generated by surveillance, and inform/consult with workers and their union about that storage, and
 - e. Inform new employees of any surveillance that is in place before they commence their employment.
5. Workers must retain the right to opt out of certain types of surveillance, including where it can be demonstrated there is a risk to workplace OHS.
6. Workers retain the right to access any data generated by any surveillance.
7. A new PIWLA must ban surveillance on workers when they are not at work, including the prohibition on social media trawling.
8. Personal data such as health data must only be collected where it is necessary for processing sick/personal leave or where legislation requires it, e.g., OHS legislation. Where it is necessary, personal data should only be collected if the worker has provided informed consent and if the employer has outlined how long it will be stored for and how the data will be destroyed.
9. Covert surveillance must not be used in any circumstances, except where it is authorised by an authority such as the police or by a warrant.
10. A new PIWLA must also enshrine a right to protection from adverse action or disciplinary action relating to data gained from surveillance.
11. There must be a ban on the disclosure or on-selling of data generated by surveillance to third parties – with the exception of where it is necessary for law enforcement agencies.

Additionally, workplace surveillance must be specifically scoped in to fall under OHS powers. The ASU supports recommendations made by Victorian Trades Hall Council:

1. New psycho-social health regulations specifically apply to the risks generated by workplace surveillance.
2. A workplace surveillance guide be produced by WorkSafe (in consultation with VTHC and unions) about how to address workplace surveillance.

The ASU also supports Victorian Trades Hall Council's proposals in regard to enforcement:

3. Fines be issued against employers who breach obligations imposed under a new PIWLA.
4. Civil remedies be available to individual workers (or groups of workers) who have suffered loss due to wrongful workplace surveillance.
5. Unions and the Wage Inspectorate Victoria have powers of investigation and to launch enforcement proceedings before the Court.