Submission No 31

INQUIRY INTO WORKPLACE SURVEILLANCE

Organisation: Australian Manufacturing Workers' Union (AMWU)

Date Received: 31 July 2024

Submission of the Australian Manufacturing Workers' Union (AMWU) to the Legislative Assembly Economy and Infrastructure Committee's Inquiry into Workplace Surveillance

31 July 2024

Australian Manufacturing Workers' Union

Stephen Fodrocy, Industrial Officer, Victorian Branch
1st Floor, 251 Queensberry Street, Carlton South VIC 3053
Telephone: (03) 9230 5700 Email: industrial.vic@amwu.org.au

Contents

1. Summary

1.1. The Australian Manufacturing Workers' Union (**AMWU**) welcomes the opportunity to make a submission to the Victorian Legislative Assembly Economy and Infrastructure Committee for its inquiry into Workplace Surveillance.

1.2. The AMWU represents around 55,000 members in every region and city in Australia. Our members manufacture, repair and maintain aircraft, defence infrastructure, mining equipment, trams, trains and buses. We process the fruit and vegetables Australia's farmers grow, we work in construction, and we maintain equipment and machinery in hospitals, buildings, factories and mines around the country.

1.3. Given the breadth of means for surveillance, the variety of workplaces (including at home, in the field and at an employer's premises) and varying nature of 'work', this submission proceeds on the basis that 'workplace surveillance' includes the listening to and recording, monitoring, observation and tracking of workers by their employers. This is not confined to situations where a worker is physically at an employer's place of business, nor confined to times when a worker is performing work for their employer. This recognises the reality of the surveillance to which our members are subject by their employers, which often extends beyond the confines of the employer's registered place of business.

1.4. The AMWU is concerned by the growing use of digital technologies for increased managerial control and surveillance, rather than used as a means to increase productivity. In some instances, workplace surveillance has the counter-productive effect of reducing productivity, for example, by adding to workers' stress and anxiety. We have also seen workplace surveillance used in ways which shifts the balance between workers and their employers, reducing control in their lives and without respect to their dignity. This greatly concerns the AMWU.

1.5. Many of our members are already experiencing significant disruption to their working lives and we expect this trend to expand into more industries as new digital technologies are adopted by employers. Workplace surveillance is of particular concern given the absence of robust protections for workers' privacy and industrial interests. The increase in the use of workplace surveillance is furthering an imbalance between employer and employees, and (worryingly) appears to be blurring the divide between the workplace and private lives (eg, where employers to monitor employees' online presence).

1.6. Examples of workplace surveillance faced by members of the AMWU include using tracking devices to determine the location of employees while on jobs and at home, engaging a third party to use facial scanning technology for clocking into work, and recording an employee while on sick leave.

1.7. While the AMWU encourages investment in new technology which will improve our members' working lives, we are deeply concerned at the expansion of surveillance of workers and its threat to the wellbeing of working people. In the absence of strong protections for workers' privacy and industrial interests, the expansion of workplace surveillance has been marred by lack of training, consultation and cooperative decision-making. Such measures would go some way to mitigate the adverse effects of workplace surveillance on Victorian workers.

2. Current Privacy and Workplace Laws on Workplace Surveillance

2.1. Current privacy and workplace laws are ineffective in protecting workers' privacy and industrial interests. There are a raft of laws and legislative materials which are engaged by workplace surveillance, providing a variety of regulatory approaches, cross-jurisdictional issues and confusing landscape for workers and employers alike.

2.2. The privacy and workplace laws which are engaged by workplace surveillance include:

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

b. The *Surveillance Devices Act 1999* (Vic) (**Surveillance Act**);

c. The *Privacy and Data Protection Act 2014* (Vic) (**Data Protection Act**);

d. The *Fair Work Act 2009* (Cth) (**Fair Work Act**); and

e. The various anti-discrimination laws.

2.3. However, these laws contain significant exemptions which undermine the protection of workers' privacy and industrial interests. It is recommended that these laws be reformed to increase the protection for workers' privacy and industrial interests, taking into account technological advancements, the expansion of the collection of information and the increased risk of unauthorised or unlawful disclosure and use.

A. The Privacy Act

2.4. The Privacy Act regulates the collection, use, disclosure and storage of personal information of individuals by organisations (companies and other entities) generally. Relevantly, an employer would be required to comply with the Privacy Act when collecting and/or disclosing personal information of an employee which has been acquired via workplace surveillance. However, an apparent exemption in relation to employee records in the Privacy Act leaves workers unprotected when it comes to workplace surveillance and their privacy.

2.5. The Privacy Act purports to provide individuals with some protection in relation to certain types of information, including (among other things): personal information (information or an opinion about an individual or someone who is reasonably identifiable);[1] health information (personal information about the health of an individual);[2] biometric information (information used for automatic verification or identification of an individual); [3] and sensitive information (which includes health information, biometric information, and personal information about an individual's political opinions, trade unionism or sexual practices).[4]

2.6. Generally, the Privacy Act prevents organisations from collecting sensitive information about an individual unless the individual consents to the collection and the information is reasonably necessary for one or more of the organisation's functions or activities (subject to some exceptions).[5] Further, the Privacy Act requires the organisation to only collect personal information by 'lawful and fair means'[6] (see, eg, below at [2.20] pursuant to the Surveillance Act or [2.40] pursuant to anti-discrimination

[1] Privacy Act s 6, definition of 'personal information'.
[2] Ibid s 6FA.
[3] Ibid s 6, definition of 'sensitive information' at sub-s (d).
[4] Ibid, definition of 'sensitive information'.
[5] Ibid s 3 of sch 1.
[6] Ibid s 3.5 of sch 1.

laws). It is noted that while the Privacy Act permits collection of personal information where an individual 'consents' to such, the notion of consent is questionable in the employment context where employees are at risk of dismissal for failing to follow their employer's directions.[7]

2.7. But for the significant exemption discussed below, the Privacy Act would prevent employers from using workplace surveillance to collect sensitive information about an employee without that employee's consent. For example, an employer would be prevented from recording visually an employee outside of work to collect about an employee's health in relation to a workers' compensation claim which the employer disputes. Employers would also be prevented from using or disclosing employee's personal information for a purpose other than the primary purpose for which it was collected, without the employee's consent. For example, an employer would be prevented from sharing photographs of its employees to a third party for the purpose of surveillance if the primary purpose for collecting the photographs was to aid clocking into work at the start of a shift.

2.8. However, acts and practices of employers are exempt from the protections in the Privacy Act in certain circumstances (the **Employee Record Exemption**).[8] The Privacy Act allows employers to collect, use and disclose personal information about an employee, if it is directly related to:

a. The employment relationship between the employer and the employee; and

b. An 'employee record' *held* by the employer.

2.9. For the purposes of the Privacy Act, an 'employee record' means a record of personal information relating to the employment of the employee.[9] The Privacy Act provides examples such as the engagement or disciplining of an employee, the employee's performance or conduct and the employee's trade union membership.

2.10. The *Explanatory Memorandum* to the Privacy Amendment (Private Sector) Bill 2000,[10] which expanded the coverage of the Privacy Act and introduced the Employee Record Exemption, indicates that the Commonwealth Government at the time had intended that the 'handling of employee records' would be 'a matter better dealt with under workplace relations legislation'. Although, the responsible minister described such information as 'deserving of privacy protection'.[11]

2.11. The Employee Record Exemption appears to leave workers significantly unprotected. Taken at is broadest, an employer would be exempt from complying with the Privacy Act in relation to any act done with an employee's personal information (including health information, biometric information, or trade union membership), to the extent that that information is directly related to the employment relationship and records held by the employer. By way of illustration, on a broad interpretation of the Privacy Act, the two examples above (at [2.7]) are likely to fall within the Employee Record Exemption, permitting an employer to collect and disclose personal information about employees by covert means and altering the balance of power between the employer and employee.

2.12. While the Employee Record Exemption only applies to employee records which are 'held' by the employer,[12] the distinction between information 'held' or 'not held' by an employer is difficult to

[7] *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946 at [14(10)], [58]; and *CFMMEU & Ors v BHP Coal* [2022] FWC 81 at [160]–[177], both cited in *Privacy Act Review: Report 2022* at 66 <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>.
[8] Privacy Act s 7B(3).
[9] Ibid s 6, definition of 'employee record'.
[10] At 5.
[11] Minister's Secord Reading Speech, Daryl Williams, Attorney-General, 12 April 2000 page 15749
[12] Privacy Act s 7B(3)(b). See, eg, *Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946.

construe. This difficulty is likely to make it complex for employers to ascertain their obligations and for employees to know their rights.

2.13. For example, it can be impractical if not impossible to ascertain what information was already held by an employer in an employee record prior to a suspected contravention of the Privacy Act, especially in circumstances where employers possess and control the relevant records at all relevant times. An unscrupulous employer, or one acting unlawfully, might falsely assert that records were held by the employer in order to evade regulatory capture.

2.14. A further issue with exempting 'held' records from protection is where the initial collection of the information forming the employee record was itself done in contravention of the Privacy Act. The Employee Record Exemption would appear on its face to sanitise the later use or disclosure of the employee's information on the basis that it is 'held' (and the other conditions are met), notwithstanding that the employer ought not to have held the information in the first place.

2.15. Similar difficulties arise when considering the requirement in the Employee Record Exemption for the information to be directly related to the employment relationship.

2.16. At its broadest, the 'employment relationship' might include any matter which arises between the employer and employee during the performance of work by the employee for that employer. This could include a record of the employee's likeness (whether by photograph or an algorithmic representation (as in biometric data)) collected by the employer, notionally for the purpose of identifying the employee at and during work. It could also include the employee's information on social media, in cases where the employer imposes restrictions on the employee's conduct outside of work, or accessing an employee's home internet service (where an employee works from home using their own devices). Seemingly, once held, the employer would be able to record covertly their employees to collect any other information directly related to both the employment relationship and the initial information.

2.17. The Employee Record Exemption raises further concerns for the consequences of workplace surveillance, specifically in relation to third parties. On one view, if the employer holds information subject to the exemption, the employer would not be prevented by the Privacy Act from disclosing that information to third parties (without the employee's knowledge or consent) and, while that disclosure must be directly related to the employment relationship, there would be little protection for the employee to affect how that third party stores, uses or discloses the information. This is because an employer would appear to be exempt from the requirement under the Privacy Act to notify an employee of (among other things) the purposes for which the information is collected and to whom the employer usually discloses that information.[13] Unless the third party itself notifies an employee that it has collected such information, an employee is unlikely to know to whom they might complain about the use, security, destruction or correction of the information (among other things).

2.18. A further issue has come to the AMWU's attention in advocating for its members under the Privacy Act. While the Privacy Act provides for 'representative applications', where a person may make an application under the Privacy Act on behalf of a class of persons, it does not lend itself to workers being represented by their union. The Privacy Act appears to require that an applicant identify themselves when making a complaint, which can be an obstacle to raising issues for many workers. Whereas, in the industrial context, unions are able to raise issues on behalf of their affected members in the Fair Work Commission, without the need to identify any members in particular.

[13] Privacy Act s 5 of sch 1.

2.19. While beyond the jurisdictional reach of the Inquiry, it is recommended that the exemptions for employee records in the Privacy Act be reviewed and amended with a view to increasing the protection for workers' privacy and industrial interests.[14] It is also recommended that processes for complaints by workers be amended to improve access to complaint resolution mechanisms.

B. The Surveillance Act

2.20. The Surveillance Act regulates the installation, use, maintenance and retrieval of surveillance devices (broadly, devices used to listen, observe, track or monitor a person or their activities),[15] including by creating offences relating to the improper installation or use of surveillance devices. While the Surveillance Act specifically deals with the use of such devices in certain parts of the workplace (eg, the washroom), the general offences are unlikely to prevent use of devices elsewhere in the workplace.

2.21. The Surveillance Act prohibits persons from (among other things) knowingly installing, using or maintaining:

a. a listening device[16] to overhear, record, monitor or listen to a private conversation (to which they are not a party) without the consent of each party to the conversation;[17]

b. an optical surveillance device[18] to record visually or observe a private activity (to which they are not a party) without the consent of each party to the activity;[19]

c. a tracking device[20] to determine the geographical location of a person or object with consent of the person or lawful possessor and/or controller of the object;[21] and

d. with regards to law enforcement officers, a data surveillance device[22] to record or monitor the input or output of computer information without the consent of the person for whom the information is being input or output.[23]

2.22. Importantly, for a person to have committed an offence with respect to [a] or [b] above at [2.21], the surveillance device must have been used in respect of a 'private activity' or 'private conversation'. As is discussed below, the definitions of which have the effect of permitting employers to use surveillance devices to monitor their workers.

2.23. Under the Surveillance Act, 'private activity' means an activity carried on in circumstances that may reasonably be taken to indicate that the parties to it desire it to be observed only by themselves, but does not include activities:

a. carried on outside a building; or

[14] See, eg, the recommendations of the *Privacy Act Review: Report 2022* at 71 <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf>.
[15] Surveillance Act s 3(1), definition of 'surveillance device'.
[16] Ibid, definition of 'listening device'.
[17] Ibid s 6.
[18] Ibid s 3(1), definition of 'optical surveillance device'.
[19] Ibid s 7.
[20] Ibid s 3(1), definition of 'tracking device'.
[21] Ibid s 8.
[22] Ibid s 3(1), definition of 'data surveillance device'.
[23] Ibid s 9.

b. carried on in any circumstances in which the parties to it ought reasonably to expect that the activity may be observed by someone else.[24]

2.24. Similarly, 'private conversation' means a conversation in circumstances that may reasonably be taken to indicate that the parties to it desire it to be heard only by themselves but does not include conversations where it would reasonably be expected to be overheard.[25]

2.25. The *Explanatory Memorandum* to the Surveillance Devices Bill 1999 provides examples of 'circumstances in which the parties to an activity ought reasonably expect that they might be observed', including 'activities in those parts of workplaces accessible to other employees or invitees of that workplace'.[26] But it is suggested that those circumstances would not include 'activities in those parts of the workplaces where the parties to the activity may exclude others from observing the activity, such as in an office with covered windows'.[27]

2.26. In short, the Surveillance Act does not prohibit surveillance of conversations or activity where it ought reasonably be expected that the conversation may be overheard or activity may be observed by persons not a party to the conversation or activity. This has significant implications for surveillance at the workplace.

2.27. Similarly, the Surveillance Act prohibits a person from using a tracking device to determine another person's location or the location of an object unless with the consent of the person or the possessor/controller of the object.[28] This provision is likely to be engaged in situations where an employer might wish to track an employee who works 'in the field'.

2.28. For example, a service technician whose work require them to travel to clients' places of business on behalf of the employer. An employer might seek to determine the employee's location by use of an electronic device on the employee and/or on a vehicle supplied by the employer to the employee.

2.29. On its face, the Surveillance Act would prevent an employer from doing tracking an employee or the vehicle without the consent of the employee (who is likely in possession and control of the vehicle). However, as is discussed above at [2.6], it is questionable whether an employee can provide free and informed consent in the employment relationship where they face the prospect of dismissal for refusing a direction of an employer.

2.30. The Surveillance Act also prohibits persons from knowingly communicating or publishing a record or report of a private conversation or activity that has been made as a result of using a listening, optical or tracking device.[29] However, a person may communicate or publish such a record or report:

a. with the consent of each party to the conversation or activity;

b. no more than is reasonably necessary for the protection of the lawful interests of the person making the communication or publication; or

c. in the course of legal or disciplinary proceedings (which are defined as proceedings under an Act of the Commonwealth, or the States or Territories);[30]

[24] Ibid s 3(1), definition of 'private activity'.
[25] Ibid, definition of 'private conversation'.
[26] At 1, cl 3.
[27] At 2, cl 3.
[28] Surveillance Act s 8(1).
[29] Ibid s 11.
[30] Ibid; s 3(1), definition of 'disciplinary proceedings'.

2.31. Assuming that the recording was obtained lawfully, a person may communicate or publish the record (or report thereof) as far as reasonably necessary for the protection of their lawful interests. This might include, for example, the interests of an employer with respect to their property, in defending against a workers' compensation claim, or asserting a contractual restriction on an employee's conduct on social media.

2.32. While the protections in the Surveillance Act appear broad enough to extend to a range of employee activities, the act contains an express protection for activities or conversations of a worker in a toilet, washroom, change room or lactation room (with some, very limited exceptions).[31] This prohibition is significantly stronger than the provisions discussed above at [2.21].

2.33. Unlike the Privacy Act, the Surveillance Act provides some more substantial protections for workers' privacy and industrial interests in relation to workplace surveillance. However, it is recommended that there is greater clarity on the circumstances which constitute private conversations and activities, and better protections for workers' legitimate interests. For example, expanding the circumstances where surveillance is expressly prohibited, such as, where a worker is exercising their rights as a health and safety representative (under the *Occupational Health and Safety Act 2004* (Vic)) and/or workplace delegate (under the Fair Work Act). Further, it is recommended that the prohibitions on the use of data surveillance should be expanded and subject to regulation beyond its use by law enforcement.

C. The Data Protection Act

2.34. The Data Protection Act applies to Victorian public sector organisations and bodies. It creates protections for personal and other information which may be held in the public sector (including public sector agencies, bodies established for a public purpose, or a contracted service provider).[32]

2.35. Relevantly, the Data Protection Act prohibits the interference with the privacy of an individual where it is contrary to or inconsistent with Information Privacy Principles (as set out in the act).[33] These principles include that an organisation: must not collect personal information unless it is necessary for its functions or activities;[34] must not use or disclose personal information for a purpose other than the primary purpose for which the information was collected (with some exceptions);[35] and must take reasonable steps to protect personal information it holds from misuse, loss and unauthorised access or loss.[36]

D. The Fair Work Act

2.36. The Fair Work Act contains several provisions which appear to involve the collection or holding of employee's information which is likely to be regulated by the Privacy Act. As is explored below at [2.44]–[2.46], the Fair Work Act would also prohibit surveillance of an employee if doing so contravened the anti-discrimination provisions of that act.

2.37. The Fair Work Act also contains a specific provision for the confidential treatment of certain information related to leave. Section 106C requires employers to take steps to ensure the confidential treatment (as far as reasonably practicable) that information concerning notices or evidence given in support of requests for personal, carer's, compassionate or family and domestic violence leave.

[31] Ibid s 9B.
[32] Data Protection Act s 13.
[33] Ibid s 16.
[34] Ibid s 1 of sch 1.
[35] Ibid s 2 of sch 1.
[36] Ibid s 4 of sch 1.

Further, employers must not (without consent of the employee) use this information for any purpose other than in satisfaction of the employee's entitlement to the leave requested.[37]

2.38. It is also noted that modern awards and enterprise agreements made pursuant to the Fair Work Act are likely to bear upon an employer's practice of workplace surveillance. For instance, an enterprise agreement might contain terms which prevent an employer from utilising workplace surveillance in relation to a particular workplace. Significantly, awards and agreements are required by the Fair Work Act to include provisions that mandate that employers must consult with employees when deciding to implement a 'major change'. If the introduction of workplace surveillance is likely to have significant impacts on employees, it is likely that it would be considered a major change upon which the employer must consult their employees. The result of that consultation might be the adoption of mitigation measures to lessen or avoid negative consequences that employees identify would flow from the introduction of surveillance technology.

2.39. While outside of the jurisdiction of this Inquiry, noting the absence of protection for employees' information in the Privacy Act (see above discussion at [2.4]–[2.19]), it is recommended that the legislation be amended to include comprehensive protections for workers' privacy and industrial interests.

E. Anti-discrimination laws (Federal and State)

2.40. Broadly speaking, an employer would be prohibited from using workplace surveillance if doing so would contravene a provision of the various anti-discrimination laws including:

a. The *Age Discrimination Act 2004* (Cth);

b. The *Disability Discrimination Act 1992* (Cth);

c. The *Racial Discrimination Act 1975* (Cth);

d. The *Sex Discrimination Act 1984* (Cth); and

e. The *Equal Opportunity Act 2010* (Vic) (**Equal Opportunity Act**).

2.41. By way of example, the Equal Opportunity Act prohibits persons from (in the case of employers) discriminating against a person in the terms on which employment is offered[38] or by subjecting an employee to detriments[39], whether directly or indirectly, on the basis of a protected attribute.[40] Those attributes include age, employment activity, industrial activity (eg, being a member of an industrial association), disability, physical features, race and sex.

2.42. Workplace surveillance would contravene the Equal opportunity Act if an employer subjected an employee to surveillance on the basis of a protected attribute. For example, if an employer subjected some employees to surveillance on racist assumptions about those employees.

2.43. In practice, it can be difficult to prove cases of discrimination because of the need to show causality between the protected attribute and the discriminating conduct. For this reason, anti-discrimination laws are unlikely to offer effective protection for employees' privacy and industrial interests, except in the cases of egregious conduct by an employer.

[37] Fair Work Act s 106C(2).
[38] Equal Opportunity Act s 16(b).
[39] Ibid s 18(d).
[40] Ibid s 6.

2.44. The Fair Work Act also offers some protection from workplace surveillance on discriminatory basis. Workplace surveillance might constitute 'adverse action' within the meaning of the Fair Work Act, where an employer discriminates between an employee and other employees by subjecting the first employee to surveillance but does not do so to other employees.

2.45. Such discrimination might contravene the Fair Work Act if, for example, that action was taken against an employee (or prospective employee) because of: the exercise of a workplace right by an employee;[41] industrial activity undertaken by the employee;[42] or a protected attribute (eg, race, gender, sexual orientation, breastfeeding, age, disability, marital status, religion, political opinion, national extraction or social origin).[43] Exceptions to the prohibition include if the adverse action is taken because of the 'inherent requirements' of the position of the employee (or prospective employee).[44]

2.46. As above with the Equal Opportunity Act, the anti-discrimination provisions of the Fair Work Act are unlikely to offer effective protection for workers' privacy and industrial interests in response to workplace surveillance. The primary difficulty is with establishing that action of an employer was taken because of a prohibited reason (eg, the exercise of a workplace right or industrial activity). While it is conceivable that an employer might record visually an employee at the workplace after the employee had lodged a workers' compensation claim (a workplace right), it is not necessarily the case that the employer did so *because* the employee lodged the claim (ie, the employer might suggest that the recording was for safety purposes or to protect their lawful interests). In the absence of proving to the requisite standard of proof, it is unlikely that the adverse action provisions of the Fair Work Act are of much assistance.

2.47. Given the difficulty identified above, it is hard to ascertain the extent to which unlawful discrimination might be involved in employers' surveillance practices. It is recommended that the State Government monitor the use of surveillance in the context of work and collect statistics which would enable it to ascertain whether such practices might involve unlawful discrimination.

[41] Fair Work Act s 340.
[42] Ibid s 346.
[43] Ibid s 351.
[44] Ibid s 351(2).

3. Current Practice of Employers

3.1. The AMWU provides the below examples to demonstrate the nature and breadth of workplace surveillance to which our members have been subjected. These examples also show the deficiencies in the regulatory framework set out above, as well as the impact that surveillance has on workers (which is explored more below).

A. Biometric Scanning to Clock In and Out

3.2. A laminate manufacturing company, with operations in Ballarat, Laminex Group Pty Ltd, implemented a system in January 2024 which required employees to submit to biometric scanning of their faces to clock in and out of work each shift, instead of the usual paper process. The company claimed that this new system was necessary because of concerns about the spread of diseases and illnesses. The new system was owned and operated by a third party.

3.3. Initially, employees were not given a choice about whether they consented to use the new system and/or provide their information to the third party. Several employees complained to the AMWU that they were worried about the security of their personal information, especially in light of the then highly publicised leak of customer information at Optus. On behalf of its members, the AMWU applied to the Fair Work Commission for resolution of a dispute arising under the enterprise agreement (relating to a failure to comply with consultation obligations) and filed a complaint with the Privacy Commissioner under the Privacy Act.

3.4. The Fair Work Commission application was resolved by consent on the basis that the company would not require its employees to use the new system and instead offer a paper-based alternative. The Privacy Commissioner complaint was discontinued by the Commissioner on the basis that it was not valid representative complaint.

3.5. The latter is an example of deficiencies in the Commonwealth laws purporting to protect workers' privacy. The company claimed that its actions were exempted under the Privacy Act on the basis of the employee record exception. Unlike an application for resolution of a dispute in the Fair Work Commission, the Privacy Commissioner appears to require individual employees to identify themselves before taking on a complaint. This clearly would have the undesirable effect of discouraging complaints by workers afraid of retaliation by their employers.

B. Unreasonable Requests for Personal and Sensitive Information

3.6. A large printing company based in Craigieburn, CCL Secure Pty Ltd, requires its employees to disclose significant personal information and the information of their domestic partners to a third party, based interstate. The types of information requested by the company include: a full birth certificate, all passports in the previous 10 years, a photograph of the employee, character references, names of family members and their birth dates, the employee's nationality and that of their family members, the name of any clubs, associations or interests groups of which they are a member, and their criminal history.

3.7. The company claims that this information is necessary for products it provides to overseas clients. There are no legislative instruments which require the company to request this information nor requiring the employees to provide the information. It is understood that the company requests this information to assist its commercial negotiations with its customers. Long-term employees report that the requirement imposed on them to provide their private information is a relatively new development, with some having worked for the company for many years before the requirement was introduced. Further, while enterprise agreement appears to demonstrate the employees have agreed

to undergo 'police criminal records' checks, it says nothing of the extensive requests for the types of information outlined above.

3.8. Several members of the AMWU complained to their union that they were worried about the security of their personal information and also uncomfortable with providing the breadth of information (personal to them and their family members), especially to third parties and, apparently, an overseas recipient.

3.9. On behalf of those members, the AMWU wrote to the company outlining its concerns in relation to the Privacy Act. This example also appears to raise potential issues under the Fair Work Act, *Racial Discrimination Act 1975* (Cth) and Equal Opportunity Act with regards to the request for the nationality of employees, their partners and their parents.

3.10. The matter remains unresolved and subject to discussions between the parties. It appears to show the problems with the existing regulatory framework, whereby workers can be coerced into consenting to provide their private information (and that of their partners and parents) or face dismissal. It is clearly questionable whether a person can truly consent to provide their personal information where they face such economic duress.

C. Realtime Monitoring and Shaming to Modify Behaviour

3.11. Members at a major, multinational company, Boeing Aerostructures Australia Limited, which manufactures for the aviation and defence industries were subject to surveillance while working on the shop floor. The company monitored the time by which workers took to complete tasks and displayed this time on screens in the workplace, accompanied by the worker's name. All passersby and other workers were able to see how long employees were taking to complete tasks.

3.12. Members complained about their health and wellbeing, including that they felt shamed into completing work at an unsafe pace, they felt it would open them to bullying or targeting by other employees, and that the practice might reduce the quality of their work. They were also concerned that the data might attract unwarranted criticism because it did not allow for nuance or explanation.

3.13. The AMWU applied to the Fair Work Commission on behalf of the affected members for the Commission's assistance in resolving the dispute. The parties were able to resolve the dispute by agreement, whereby the company would no longer display the workers' names and communicate with the relevant team with respect to their concerns.

3.14. This case example demonstrates how the use of new technologies and data collection can be used to alter the balance of power between employees and employers, and the impact employers' practices can have on the wellbeing of workers. The affected workers at this company are highly skilled and experienced, and the work they perform requires a high level of attention otherwise there could be serious and significant consequences for the safety of customers and users of the product. The introduction of the monitoring tool paid little regard to the workers' skills and experience because it displayed the data without context or explanation. This devalued the expertise of the workers and subjected them to feelings of shame and distress. While the parties were able to resolve the dispute using the mechanisms in the relevant enterprise agreement, there is little protection outside of that instrument in the regulatory framework generally.

D. Monitoring and Tracking Employees in the field

3.15. Members at multiple companies (ranging from on-call automotive support at RACV to repair technicians operating on location for Asahi Beverages Pty Ltd) are subject to GPS tracking and camera recording in their work vehicles, which they are entitled to use for reasonable personal use. There is

little protection for the members' personal information that collected at times when they use these vehicles personally.

3.16. For example, workers at RACV providing on-call automotive support are entitled to take their work vehicles home. The vehicles are fitted with GPS tracking devices, the members are not permitted to disconnect those devices when not on the job. Additionally, the company has started installing multiple cameras in and on the vehicles, which record workers inside the cabin (and outside) while the vehicles are turned on and remain recording for around three hours after workers turn off their vehicles. Because of the nature of the work, employees may need take their meal and bathroom breaks while inside the car (this raised concerns with regard to s 9B of the Surveillance Act, above at [2.32]). It also appears that the company is using third party software to analyse the data recorded by the cameras to monitor workers' movements and send notifications to the company.

3.17. The introduction of these measures at RACV will be subject to consultation where workers intend to raise their concerns. Some of their concerns include that their movements are being recorded extensively both while at work and afterwards (including on meal and bathroom breaks), representing a violation of their dignity and privacy. The members have raised their concern that the data collected will be used against them unfairly and unreasonable for disciplinary action. They are also significantly concerned about the impact that the constant monitoring will have on their mental health and well-being. Further, they have unanswered questions about how the data is stored and protected, who owns or has possession of that data, and the purposes for which the data might be used.

3.18. The union has acted on behalf of its members affected by practices of this kind, but we have found the regulatory framework wanting when it comes to protecting workers' privacy and industrial interests. The balance of interests appears to be weighed in favour of the employer's proprietary rights, at the expense of the workers' rights to privacy and their industrial rights. It is understandable that the employers have a legitimate interest in seeking to protect their property, but we consider that there are reasonable protections which could be introduced in respect of workers, which would not fundamentally detract from employers' legitimate concerns.

3.19. As is explored below, the AMWU considers that the introduction and use of surveillance technology should involve cooperative decision-making with affected workers, transparency and accountability around the purpose, use and misuse of the technology, stronger regulation around the storage and retention of information acquired through the technology, and regular audits and reviews to analyse the continuing need for using the surveillance technology.

E. Surveillance of a Worker on Sick Leave

3.20. A sales representative for a large multinational car company was subject to surveillance by his employer while he was on sick leave suffering from an injury he had incurred at work.

3.21. During proceedings made on behalf of the member, the company revealed that it had spied on the worker while he was on sick leave. The surveillance included recording him outside his home and at family members' houses. The company attempted to use this information as apparent evidence supporting its allegations against the worker that he had misrepresented his illness. The information was collected without the member's knowledge or consent.

3.22. The worker was seriously affected when he found out that the company had been recording him while he was off sick. He reported experiencing feelings of anxiety, insult and violation. Not only did these practices make it more difficult in reaching a resolution to the proceedings against the company but they are also likely to have worsened the worker's mental health and well-being.

3.23. As was explored above, the current Surveillance Act would not provide the worker protection from the collection and use of this information because it related to the worker's activities 'outside of a building'. However, the case is an extreme example of the lengths that some employers may go to when using surveillance technology against their workers.

3.24. The AMWU considers this an important example of employer practices primarily because it relates to surveillance outside of the workplace (ie, the employer's usual place of business). We are concerned by employers monitoring and recording workers' activities outside of the strict confines of the workplace, and we encourage the Inquiry not to limit its examination to a restrictive conception of the 'workplace'. While we have not presented examples of employers monitoring their workers' online activities, we know that many workers face these practices in many industries operating in Victoria.

4. Collection, Sharing, Storage, Disclosure and Disposal of Data

4.1. From the examples above, it is apparent that employers are using various methods to collect, share, store and disclose surveillance data. However, little information is known about how such data is disposed or sold, which is an enduring concern to the AMWU.

4.2. In our experience, employers have used covert methods to collect data (in the case of the sales representative above at [3.19]), overt methods (in the case of the aviation and defence company, above at [3.11]), remote methods (in the case of GPS tracking of vehicles, above at [3.15]), digital methods (in the case of biometric scanning, above at [3.2]) and analogue methods (where members were asked to provide information directly, above at [3.6]).

4.3. In the case of the biometric scanning, the company involved stated that the data would be stored digitally by the third party, on its services. That third party provided some information (through the employer) about the apparent safeguards it had in place to secure the stored data. This also raised concerns about the location of the server on which the data was stored, for example, whether it was located in Australia or elsewhere (which would have relevance for the protections under the Privacy Act). Further, the same third party did not appear to reveal to whom it would disclose the data or for what purpose. This raised concerns that the data might be shared with other parties for unknown purposes (eg, marketing and/or demographic profiling), and/or to parties undesirable to the workers (eg, political parties or lobbying groups with which the workers disagree).[45]

4.4. Given that the Surveillance Act appears to allow employers to record covertly their employees (in certain circumstances), it is concerning that the Privacy Act appears to exempt such records from its obligations with regard to notification of collection, destruction and/or de-identification of information where it is no longer required, and from taking steps to protect information from misuse, interference and loss.

[45] Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested by Cambridge Analytica in major data breach' (The Guardian (online), 18 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

5. The Privacy, Autonomy and Dignity of workers

5.1. There appears to be little protection for the workers' interests within the existing regulatory framework. While there are various laws and schemes which might apply to regulate workplace surveillance, their implementation is difficult in practice.

5.2. As is always the case, the regulation of workers' interests to privacy, autonomy and dignity is balanced against the proprietary and commercial interests of their employers. In our view, the balance is skewed in favour of the employers.

5.3. Using the aviation and defence company's case as an example (see above at [3.11]), workers were made to feel shamed and distressed because of a desire by their employer to use surveillance technology to improve productivity. In our view, this was likely to be counterproductive because workers felt pressured to increase the pace of their work, foregoing concerns for quality. Given the nature of their work, precision and accuracy ought to be important concerns for the company. Members in this industry are highly skilled and trained. They are called on to apply those skills in a challenging environment, working on precise and technical parts which, if faulty, could have serious safety effects.

5.4. By emphasising speed and quantity, the introduction of surveillance and monitoring restrained the workers' autonomy to apply their skills to the work according to their experience and training. Similarly, by allowing for direct comparisons between workers, the displaying of each person's productivity on the shop floor caused significant indignity to the workers. The result was an alienation and atomisation of the workers from each another, because the information necessarily invited comparison and competition among them. The consequence was dehumanising and devaluing for the workers affected. The AMWU considers this fact alone to warrant greater protection for workers' privacy and industrial interests.

5.5. The various examples above (and the many others known to the AMWU) demonstrate the impact that surveillance in the work context has on Victorians. The case of the sales representative demonstrates an important factor in support of greater protection for workers' privacy and industrial interests, that feeling of being violated by surveillance practices and the real harms which follow. The exemptions and exceptions in the regulatory framework which allow employers to collect and use personal information about their workers is fundamentally about prioritising the employers' economic, proprietary and commercial interests above the protection of workers' autonomy, dignity and well-being. We urge the State Government to intervene to reset the balance urgently, as new technologies emerge and employers increasingly adopt new and sophisticated ways of surveillance.

6. The Personal Impact of Workplace Surveillance

A. Physical and Mental Safety

6.1. Workplace surveillance can significantly impact the physical and mental health of workers. Research shows that continuous monitoring can lead to increased stress levels, anxiety, and other mental health issues. Surveillance can create a sense of being constantly watched, which can lead to heightened stress responses and feelings of invasion of privacy (see, eg, above at [3.19]). This stress can manifest physically, leading to conditions such as headaches, high blood pressure, and sleep disturbances.

6.2. Studies have found that employees subjected to high levels of surveillance report greater psychological distress and lower job satisfaction. The constant pressure to perform under surveillance can exacerbate pre-existing mental health conditions or contribute to new ones, such as depression and anxiety.[46]

B. Stress and Productivity

6.3. The relationship between surveillance, stress, and productivity is complex. While employers may implement surveillance with the intention of boosting productivity, the opposite effect is often observed (see, eg, above at [3.11]). High levels of stress induced by surveillance can impair cognitive function, reduce job satisfaction, and ultimately decrease productivity.

6.4. A systematic review of workplace stress highlighted that surveillance often leads to a decrease in worker autonomy and trust, which are crucial for a productive work environment.[47] The review also found that surveillance could result in higher turnover rates and lower organisational commitment.[48]

C. Recommendations

6.5. To mitigate the negative impacts of workplace surveillance on workers' health and well-being, the following policies are recommended:

a. **Transparent Surveillance Policies**: Employers should clearly communicate the extent and purpose of surveillance to employees. Transparent policies can help reduce anxiety and build trust between employees and employers.

b. **Employee Consent and Participation**: Involve employees in the design and decision-making process regarding surveillance practices. Ensuring that employees have a say in how surveillance is conducted can enhance their sense of control and reduce stress.

c. **Regular Mental Health Assessments**: Implement regular mental health check-ins and provide access to mental health resources. This can help in early identification and management of stress-related issues.

---

[46] T Cheung and PSF Yip, 'Depression, anxiety and symptoms of stress among Hong Kong nurses: a cross-sectional study' (2015) 12(9) *International Journal of Environmental Research and Public Health* 11072 <https://www.mdpi.com/1660-4601/12/9/11072>.

[47] Gabriella Maria Schr Torres et al, 'A Systematic Review of Workplace Stress and Its Impact on Mental Health and Safety' (Conference Paper, SpringerLink, 2020) <https://link.springer.com/chapter/10.1007/978-3-031-48041-6_41>.

[48] American Psychiatric Association, 'Stigma, Prejudice, and Discrimination Against People with Mental Illnesses' (WebPage, March 2024) <https://www.psychiatry.org/patients-families/stigma-and-discrimination>.

d. **Limiting Surveillance Scope**: Restrict surveillance to only necessary areas and avoid intrusive monitoring. For example, limiting surveillance to work-related activities and avoiding personal spaces can help protect workers' privacy.

e. **Supportive Work Environment**: Create a supportive work environment that prioritises employee well-being. Encourage open communication, provide stress management resources, and promote a healthy work-life balance.

6.6. By adopting these measures, employers can create a healthier work environment that respects workers' privacy and dignity while maintaining productivity.

7. The Impact of on Power Dynamics and Workplace Relations

A. Power Dynamics

7.1. Workplace surveillance significantly shifts the power dynamics between employers and employees. The constant monitoring and data collection capabilities afforded by modern surveillance technologies give employers an unprecedented level of control over workers. This imbalance can manifest in various ways, including the ability to track employee performance, behaviour, and even personal data, which can be used to influence workplace decisions and policies.

7.2. A study by the London School of Economics highlights that surveillance technologies, such as remote monitoring and biometric data collection, allow employers to gather extensive data on employees' activities and health (see above discussion on the Privacy Act in relation to health information at [2.5], [2.7], [2.11]). This data can be used not only for performance evaluations but also for making predictive decisions about an employee's future behaviour and productivity, often without the employee's knowledge or consent. Such practices can erode employee autonomy and exacerbate the power imbalance in the workplace, leading to a sense of constant scrutiny and potential job insecurity.[49]

B. Workplace Relations

7.3. Surveillance can severely impact trust and cooperation within the workplace. When employees feel they are being constantly monitored, it can lead to a breakdown in trust between them and their employers. This erosion of trust can diminish the sense of mutual respect and cooperation, which are essential for a productive and positive work environment.

7.4. Research from the European Foundation for the Improvement of Living and Working Conditions (**Eurofound**) indicates that the increased capacity for gathering and recording data about workers' performance and behaviour can heighten the risk of privacy breaches and damage trust in management. This distrust can negatively affect job satisfaction and the overall quality of workplace relations.[50] Furthermore, constant surveillance can create a work culture where employees feel undervalued and treated as mere tools for productivity, rather than as trusted members of the organisation.[51]

C. Recommendations

7.5. To mitigate the negative impacts of workplace surveillance on workplace relations and balance of power, the following measures are recommended:

a. **Transparent Policies**: Employers should develop and implement clear and transparent surveillance policies that are communicated to all employees. This includes specifying the purpose, scope, and methods of surveillance, as well as how the collected data will be used.

---

[49] Sara Riso, 'Monitoring and Surveillance Technologies Shift Power Dynamics in the Workplace' (WebPage, European Foundation for the Improvement of Living and Working Conditions, 31 July 2024) <https://www.eurofound.europa.eu/en/monitoring-and-surveillance-workers-digital-age>;Aiha Nguyen, 'Monitoring and Surveillance Technologies Shift Power Dynamics in the Workplace.' (Blog, London School of Economics, 5 March 2019) <https://blogs.lse.ac.uk/businessreview/2019/03/05/monitoring-and-surveillance-technologies-shift-power-dynamics-in-the-workplace/>.

[50] Above n 49.

[51] Jessica Vitak and Michael Zimmer, 'Surveillance and the Future of Work' (2023) 28(4) Journal of Computer-Mediated Communication <https://academic.oup.com/jcmc/article/28/4/zmad007/7210235>; Alex Rosenblat et al, 'Workplace Surveillance' (Working Paper, Data & Society, 8 October 2014) <https://www.datasociety.net/pubs/fow/WorkplaceSurveillance.pdf>.

b. **Employee Involvement**: Involve employees in the design and development of surveillance policies and practices. Providing a platform for employee input can enhance their sense of control and participation, thereby reducing feelings of powerlessness and distrust.

c. **Privacy Protections**: Implement strict data protection measures to safeguard employees' personal information. This includes limiting the collection of data to what is strictly necessary for business operations and ensuring that data is used ethically and responsibly.

d. **Regular Audits and Reviews**: With employees, conduct regular audits and reviews of surveillance practices to ensure they comply with legal standards and ethical norms. This can help identify and rectify any practices that may infringe on employees' rights and privacy.

e. **Supportive Work Environment**: Foster a supportive work environment that prioritises employee well-being. Encourage open communication and provide resources for stress management and mental health support.

7.6. By adopting these measures, organisations can help balance power dynamics, protect employees' privacy, and foster a more trusting and cooperative workplace environment.

8. The Impact on Workers' Rights and Existing Legal Protections

A. Workers' Rights

8.1. Workplace surveillance can infringe upon several fundamental workers' rights, including the right to privacy, freedom of association, and protection from discrimination (see above at [2.4], [2.36] and [2.40]).

8.2. Surveillance technologies, such as AI-driven productivity tools, biometric monitoring, and constant digital tracking, can create environments where a worker's every move and behaviour is monitored and recorded.[52] This level of monitoring often extends beyond the workplace, intruding into personal lives and blurring the line between work and private time.

8.3. Surveillance can also impact workers' rights to organise and engage in collective bargaining. For instance, the National Labor Relations Board in the United States has warned that AI-enabled surveillance of labour organising activities might violate rights protected under the *National Labor Relations Act*, 29 USC §§ 151–169 (2024).[53] This infringement can deter workers from participating in union activities due to fear of retaliation or job loss.

B. Legal Protections

8.4. Current legal protections for workers' rights in the context of surveillance vary widely and are often insufficient (see above discussion at section 2). In many jurisdictions, laws lag behind technological advancements, leaving significant gaps in protection. For example, while some laws provide basic privacy protections, they may not cover newer forms of digital and biometric surveillance comprehensively (see, eg, above at [2.21], in relation to the Surveillance Act and tracking devices).

8.5. The General Data Protection Regulation in the European Union offers one of the more robust frameworks, emphasising principles like data minimisation and purpose limitation. However, enforcement and applicability can be inconsistent, especially in complex work environments involving remote or gig work.[54]

8.6. In the United States, legal protections are less comprehensive. While there are federal and state laws addressing certain aspects of workplace privacy and discrimination, these laws often do not fully address the invasive nature of modern surveillance technologies. For example, the *Electronic Communications Privacy Act*, 18 USC §§ 2510–2523 provides some protections, but its applicability to workplace surveillance is limited, and it does not cover all types of monitoring.

C. Recommendations

8.7. To enhance the protection of workers' rights in the context of workplace surveillance, several measures can be recommended:

---

[52] Aiha Nguyen, *The Constant Boss*, (Data & Society, May 2021) < https://datasociety.net/library/the-constant-boss/>; Merve Hickok and Nestoer Maslej, 'A Policy Primer and Roadmap on AI Worker Surveillance and Productivity Scoring Tools', (2023) 3 *AI and Ethics* 673 <https://link.springer.com/article/10.1007/s43681-023-00275-8>.

[53] J Abruzzo, 'Labor Organizing and AI Surveillance in the Workplace' (Memo, 31 October 2022) *Office of the General Counsel of the National Labor Relations Board* <https://apps.nlrb.gov/link/document.aspx/09031d45838de7e0>.

[54] London School of Economics, 'Monitoring and surveillance technologies shift power dynamics in the workplace' (Blog, 16 March 2019) <https://blogs.lse.ac.uk/usappblog/2019/03/16/monitoring-and-surveillance-technologies-shift-power-dynamics-in-the-workplace/>.

a. **Strengthen Privacy Laws**: Update and expand privacy laws to cover all forms of digital and biometric surveillance comprehensively. This includes ensuring that employees are fully informed about surveillance practices and have the ability to freely consent or opt-out.

b. **Transparency and Accountability**: Employers should be required to provide clear, transparent information about the nature, purpose, and scope of surveillance. Regular audits and reporting on surveillance practices can help ensure accountability.

c. **Limit Surveillance Scope**: Implement strict limitations on the scope of surveillance to ensure it is proportional and necessary for legitimate business purposes. Surveillance should not extend into personal time or activities unrelated to work.

d. **Protect Collective Rights**: Safeguard the rights to organise and engage in collective bargaining by prohibiting surveillance practices that monitor or interfere with union activities. Strengthen protections against retaliation for participating in such activities.

e. **Implement Worker Protections**: Introduce measures to protect workers from discrimination and unfair treatment based on data collected through surveillance. Ensure that surveillance data is not used in ways that disadvantage certain groups of workers disproportionately.

f. **Data Security and Retention**: Establish robust data security protocols to protect the information collected through surveillance. Implement strict data retention policies to ensure that data is not kept longer than necessary and is disposed of securely.

8.8. By adopting these measures, policymakers can better protect workers' rights in the face of increasing surveillance and ensure a fairer, more equitable work environment.

9. Summary of Recommendations

9.1. Investment in new technology is an essential component of protecting Victoria's strong industrial base and the quality of life for working people. However, the AMWU remains concerned at the apparent trend with regard to the use of surveillance technology to monitor our members. Our experience suggests that the use of such technology is negatively affecting the safety and wellbeing of workers, unreasonably infringing upon their rights including to privacy and industrially, worsening the imbalance of power between workers and their employers, and encroaching upon workers' private lives.

9.2. The AMWU contends that, in the absence of strong protections for workers' privacy and industrial interests, the incidence of workplace surveillance in Victoria has involved a distinct lack of training, consultation and cooperative decision-making. We believe such measures would go some way to mitigate the adverse effects of workplace surveillance on Victorian workers.

9.3. In summary, the AMWU recommends that the State Government:

a. Explores ways in which it might improve the protection of workers' privacy in a manner which is not inconsistent with the Federal Privacy Act, including establishing robust requirements for the data security and retention;

b. Improves the protections in the Surveillance Act to provide for better protection of workers' legitimate interests and rights;

c. Considers expanding the prohibition and regulation of the use of data surveillance to accord with modern use of such technologies;

d. Monitors the use of surveillance in the work context and collects statistics which would enable it to ascertain whether such practices might involve unlawful discrimination and ensures that information is not used in ways that disadvantages groups of workers disproportionately;

e. Introduce legal requirements for employers to mitigate the impact of surveillance including to ensure transparency, require worker consent and participation, adopt regular mental health assessments, limit the scope of use, encourage a supportive work environment, and require regular audits and reviews; and

f. Reviews the protections for collective rights (such as union activities) from surveillance practices and explores ways in which it might improve such protections in a manner which is not inconsistent with the Federal Fair Work Act.