Legislative Assembly
Economy and Infrastructure Committee

Inquiry into workplace surveillance

May 2025

Published by order, or under the authority, of the Parliament of Victoria
May 2025

ISBN 978 0 908262 22 9 (print version)
ISBN 978 0 908262 23 6 (PDF version)
This report is available on the Committee's website: parliament.vic.gov.au/eic-la

Committee membership

CHAIR
Alison Marchant
Bellarine

DEPUTY CHAIR
Kim O'Keeffe
Shepparton

Roma Britnell
South-West Coast
(From 30 October 2024)

Anthony Cianflone
Pascoe Vale

Wayne Farnham
Narracan
(Until 28 November 2024)

John Mullahy
Glen Waverley

Nicole Werner
Warrandyte
(From 28 November 2024)

Dylan Wight
Tarneit

Jess Wilson
Kew
(Until 30 October 2024)

About the Committee

Functions

The Committee is established under the Legislative Assembly Standing Orders and can examine any matters or issues connected with these departments and their related agencies:

- Department of Education
- Department of Jobs, Skills, Industry and Regions
- Department of Transport and Planning
- Department of Treasury and Finance.

Secretariat

Kerryn Louise Riseley, Committee Manager
Dr Marianna Stylianou, Research Officer
Abbey Battista, Administrative Officer
Patrick Horan, Law student (5 June to 7 August 2024)

Contact details

Address Legislative Assembly Economy and Infrastructure Committee
Parliament of Victoria
Parliament House, Spring Street
East Melbourne Victoria 3002

Phone +61 3 8682 2822

Email eic.assembly@parliament.vic.gov.au

Web parliament.vic.gov.au/eic-la

Contents

Preliminaries

Committee membership ii
About the Committee iii
Terms of reference ix
Chair's foreword xi
Executive summary xiii
Findings and recommendations xvii
Acronyms and terms xxiii
Figures xxv
Tables xxvi
Case studies xxvii

1 Introduction 1

1.1 Workplace surveillance is more sophisticated and far-reaching now 2
1.1.1 Employers can use a wide range of surveillance methods 3
1.1.2 There are legitimate reasons for workplace surveillance 5
1.1.3 Workplace surveillance can collect a vast amount of data 7
1.1.4 Workplace surveillance laws in Australia are inconsistent 8
1.1.5 There is growing interest in the legal frameworks around workplace surveillance 12
1.2 Scope of the Inquiry 15
1.3 Inquiry process 16
1.4 Report outline 16

2 Workplace surveillance practices in Victoria 19

2.1 Workplace surveillance is growing in Victoria 19
2.1.1 Victorian employers use a wide range of surveillance practices 19
2.1.2 Technology and remote work have fuelled the rise in workplace surveillance 22
2.2 Artificial intelligence is increasingly used in workplace surveillance 27
2.2.1 Using AI with workplace surveillance has risks of bias and unfairness 30

2.3 Victorian employees are rarely informed about surveillance practices 32
2.3.1 Victorian employees are unaware of the full extent of workplace surveillance 33
2.3.2 Undisclosed function creep is problematic 35

3 Impacts of workplace surveillance 41
3.1 There is little evidence to suggest surveillance improves productivity 41
3.2 Intrusive surveillance can produce a toxic workplace culture 45
3.3 Surveillance intensifies work creating health and safety risks 48
3.4 Workers' health can be harmed by constant surveillance 50
3.5 Surveillance can breach the privacy of workers and their families 54
3.6 Surveillance can exacerbate the power imbalance in the workplace 58
3.7 Workers are less likely to take collective action when surveilled 59
3.8 The impact of workplace surveillance is worse for some workers 61

4 Regulation of workplace surveillance 65
4.1 Workplace surveillance laws in most jurisdictions are inadequate 65
4.1.1 Current Victorian workplace surveillance laws are ineffective 66
4.1.2 Workplace surveillance laws in NSW and ACT are better but also have failings 71
4.1.3 Federal laws do not specifically cover workplace surveillance 75
4.1.4 Workplace surveillance laws overseas offer varying levels of protection 77
4.1.5 There are no international conventions specifically on workplace surveillance 79
4.1.6 There are several principles that should guide best-practice regulation 81
4.2 Victoria's workplace surveillance laws need modernising 83
4.2.1 The Fair Work Act preserves Victoria's power to regulate workplace surveillance 85
4.2.2 Safeguards around workplace surveillance must be enhanced 85
4.2.3 Workers also need protection against surveillance by third parties 99

5 Surveillance data and employee privacy 103

5.1 Employers' data handling is not transparent risking workers' privacy 103

5.1.1 Workers are left in the dark about how their data is used, shared and stored 104

5.1.2 Privacy and data security threats escalate as workplace surveillance grows 107

5.2 Current privacy laws are ineffective at protecting workers' data 109

5.2.1 Victoria's privacy laws are limited to the public sector 109

5.2.2 ACT is the only Australian jurisdiction to protect workplace surveillance data 112

5.2.3 Employee records and small businesses are exempt from the federal Privacy Act 113

5.2.4 The European Union has robust data protection laws 115

5.2.5 The International Labour Organization guides the protection of workers' data 117

5.2.6 Best-practice data protection is transparent and accountable 118

5.3 Data protection in Victoria can be strengthened 119

5.3.1 The first round of Privacy Act reforms do not alter how employee data is treated 120

5.3.2 Expanding Victoria's privacy protections will reduce data security risks 121

5.3.3 A regulator should be appointed to oversee workplace surveillance 129

6 Conclusion 133

Appendix

A About the Inquiry 135

Glossary 141

Bibliography 143

Extracts of proceedings 151

Minority report 155

Terms of reference

Inquiry into workplace surveillance surveillance

On May 14 2024, the Legislative Assembly agreed to the following motion:

That this House refers an inquiry into the extent to which surveillance data is being collected, shared, stored, disclosed, sold, disposed of and otherwise utilised in Victorian workplaces to the Economy and Infrastructure Standing Committee for consideration and report no later than 31 March 2025 including, but not limited to, an examination of:

(1) The effectiveness of current privacy and workplace laws when it comes to employee workplace surveillance;

(2) The current practices of employers disclosing the use of workplace surveillance to employees and others;

(3) The manner in which surveillance data is collected, shared, stored, disclosed and disposed of or sold, including but not limited to covert, overt, remote, digital and analogue methods;

(4) The ownership of workplace surveillance data;

(5) The protection of the privacy, autonomy and dignity of workers and other individuals, and the potential for privacy and data security risks to individuals, workers, businesses, communities and Victoria;

(6) The personal impact of workplace surveillance on Victorian workers, such as on their physical and mental safety;

(7) The impact of workplace surveillance on workplace relations and the balance of power between employers and workers;

(8) The impact of workplace surveillance on the balance of power in the workplace and the effect on workers' rights;

(9) International or domestic examples of best practice workplace surveillance regulation and privacy protection;

(10) The potential consequences of unregulated surveillance on workers and their families;

(11) Australia's obligations under international law, including International Labour Organization Conventions;

(12) The interaction between State and Commonwealth laws, and the jurisdictional limits imposed on the Victorian Parliament; and

(13) Any other related matters.

On 4 February 2025, the Legislative Assembly passed a motion extending the reporting date for the Inquiry to 30 April 2025.

Chair's foreword

I am pleased to present this report on the Inquiry into workplace surveillance.

Workplace surveillance has accelerated in recent years in Victoria and indeed worldwide as a result of technological advancements and the shift towards remote working. In a short space of time, surveillance has advanced beyond camera footage and the recording of telephone calls to incorporate keylogging, wearable trackers, biometrics, neurotechnology and artificial intelligence. Over this time, our privacy and surveillance laws have not kept pace in Victoria.

It became clear throughout the Inquiry that many Victorian workers are unaware of the extent of surveillance in their workplace and how their employers are handling and storing data collected through workplace surveillance. Existing Victorian and federal legislation provide minimal protection of workers' privacy, and the lack of safeguards were highlighted by experts and workers.

While there are legitimate reasons for employers to undertake surveillance, such as to ensure workers' health and safety, it can become problematic when employers use surveillance covertly for other purposes. This can raise privacy concerns and cause distress for employees when their employer's surveillance practices are unreasonable or excessive.

Workplace surveillance that is excessive and lacks transparency has been shown to have a negative impact on employees' morale, job satisfaction and commitment to their organisation. It has also been shown that it can intensify work, adversely affect employees' mental and physical health and exacerbate the power imbalance between employers and employees.

After considering best-practice regulation interstate and overseas, the Committee recommends Victoria introduce new workplace surveillance laws that are technology neutral and ensure surveillance is reasonable, necessary and proportionate to achieve a legitimate objective. Victorian employers should be required to notify and consult with workers about workplace surveillance practices and disclose how workers' data will be collected, used and stored.

This Inquiry was held at the same time as reforms to the federal Privacy Act were underway. The first tranche of reforms to the Act passed in late 2024 and did not address workplace surveillance. While future reforms may have implications for workplace surveillance, there is no guarantee when these changes will be made and if they will provide effective safeguards considering the Act does not specifically deal with workplace surveillance but with information privacy. For this reason, the Committee felt that Victoria should not wait to strengthen protections around workplace surveillance but instead lead the way with dedicated, principles-based legislation.

On behalf of the Committee, I thank the organisations and individuals who made submissions and attended public hearings to provide their views and expertise. We greatly appreciate the time and effort of all who contributed as their evidence enhanced our understanding of current workplace surveillance practices and where regulatory gaps currently exist. The Committee did seek input from large employers and companies but only one made an individual submission, none accepted the invitation to attend a public hearing and only one responded to questions in writing. We therefore appreciated the representation from peak bodies and industry groups.

I extend my thanks to the Deputy Chair, Kim O'Keeffe MP, and my fellow past and present Committee Members who worked on this Inquiry—Roma Britnell MP, Anthony Cianflone MP, Wayne Farnham MP, John Mullahy MP, Nicole Werner MP, Dylan Wight MP and Jess Wilson MP.

I also wish to thank the Secretariat, Kerryn Riseley, Marianna Stylianou and Abbey Battista, for their diligence and dedication in preparing this report.

Alison Marchant MP
Chair

Executive summary

Employers monitoring employees via optical, listening, computer or tracking devices is growing in popularity in workplaces around the world, including in Victoria. Surveillance technology has become more sophisticated, affordable and easy to use over the past two decades, yet Victoria's workplace surveillance laws have not changed since 2006, suggesting that regulation has not kept pace with modern practices.

The Legislative Assembly's Economy and Infrastructure Committee was asked to examine the effectiveness of existing workplace surveillance and privacy laws, the impact of workplace surveillance on workers and workplace relations, potential privacy and data security risks, and best-practice regulation interstate and overseas.

The Committee heard about the legitimate reasons for workplace surveillance but also the potential negative impacts on workers, organisational culture and workplace relations if surveillance is unreasonable or excessive. The evidence clearly showed that current state and federal laws are ineffective at regulating workplace surveillance and protecting employees' privacy and rights.

Workplace surveillance is becoming more common in Victoria

Optical and listening surveillance at work have a long history. Now, devices such as computers, webcams, mobile phones and handheld scanners gather data on work activities that can be processed and used to determine workers' location and task speed and assess their performance, sentiment and concentration level. Newer technologies have enabled more sophisticated surveillance that collects data at a greater and more granular scale. In addition, employers are using artificial intelligence to process workplace surveillance data and reach conclusions about workers' behaviour, sentiment and performance using algorithms that are not transparent and could be biased. In some instances, automated decision-making is triggering disciplinary processes and dismissals.

The rise in remote working following the COVID-19 pandemic lockdowns led to a surge in demand for surveillance software. While employers needed assurance that the person accessing company systems was a genuine worker, the speed at which the software was rolled out gave employers little time to consider the legal and privacy implications and employees did not have enough information about how the software works to challenge its adoption.

The Committee heard that Victorian employers are seldom transparent with employees about the extent and manner of their workplace surveillance practices, leaving most workers unaware of how employers, or even contracted third parties, collect, use and handle their data. Furthermore, unions and workers are concerned about function creep, where employers use surveillance deployed for a specific reason, such as safety, for other purposes, such as performance management, without informing employees.

Intrusive workplace surveillance has a range of negative impacts

Employers have legitimate reasons for using surveillance such as protecting property and workers' health and safety as well as other reasons such as improving work processes. Research is inconclusive about the impact of workplace surveillance on productivity; however, it has been shown to decrease job satisfaction, increase stress and strain, and negatively affect employees' wellbeing and work attitudes, which are factors known to lower productivity. When employees feel that workplace surveillance is intrusive or their employers are not being transparent about it, they are less likely to trust their managers and are less committed to their organisation, resulting in disengagement, poor workplace culture and increased staff turnover.

While workplace surveillance can help to protect workers' safety, it can also have a negative impact on health and safety through work intensification. Constant monitoring places pressure on employees to work harder and faster and take fewer breaks and potentially risky shortcuts. This may affect workers' physical health through workplace accidents and injuries, and also upset their mental health through stress and anxiety if they feel constant surveillance is excessive or unjust.

There is also an impact on workplace relations because surveillance exacerbates the power imbalance between employers and employees, especially when employees feel they cannot object to it without negative consequences such as losing their job. Furthermore, workers are hesitant to take collective action if they feel their movements and communications with other workers or union officials are being monitored.

Workplace surveillance also poses a risk to workers' privacy and that of their families and community members who may be captured by surveillance devices outside of the workplace such as at home or in a work vehicle. The potential harms of workplace surveillance are felt more intensely by workers who are marginalised, more likely to work in highly monitored workplaces, and have weaker bargaining positions, such as women, young people, migrants and platform workers.

Victorian and federal laws are ineffective at regulating workplace surveillance

Victoria's laws have not kept pace with the technological advances and growth of surveillance devices in the workplace. The *Surveillance Devices Act 1999* (Vic) prohibits optical and listening surveillance in workplace toilets, washrooms, change rooms and lactation rooms, and requires consent for location tracking and the recording of private activities and conversations. However, the way these terms are defined in the Act means that most instances of workplace surveillance do not fall within its scope. In addition, the Act only addresses data surveillance in terms of its use by law enforcement officers, which demonstrates how outdated the law is when surveillance by computers is one of the most common forms of workplace surveillance used in Victoria today.

New South Wales and the Australian Capital Territory (ACT) are the only Australian jurisdictions to have dedicated workplace surveillance laws. They require employers to give employees advance notice of how and when surveillance will take place. The ACT also requires employers to state the purpose of the surveillance, consult with employees about introducing surveillance, and protect the surveillance data they collect. While offering more protections than the Victorian legislation, these laws have not been updated recently, do not cover all surveillance technologies, and are based on a consent model, which is inappropriate in a workplace context if objecting results in the worker's dismissal.

Federal laws do not address workplace surveillance and therefore provide minimal safeguards. In fact, the *Fair Work Act 2009* (Cth) preserves the states' powers to regulate workplace surveillance. The *Privacy Act 1988* (Cth) exempts employee records and small businesses from compliance with its privacy requirements, leaving many workers unprotected. There are also no legally binding international conventions regulating or prohibiting workplace surveillance that Australia must adhere to.

According to academics and information commissioners in Australia and overseas, best-practice regulation of workplace surveillance incorporates the principles of reasonableness, necessity, proportionality, fairness, transparency and data minimisation. The Committee recommends that Victoria introduce new principles-based workplace surveillance laws that are technology neutral and require employers to show that any surveillance they conduct is reasonable, necessary and proportionate to achieving a stated legitimate objective. Employers should also notify workers of surveillance, specifying the methods, scope, timing and purpose of the surveillance and how the data will be used and stored, and consult with employees before introducing or changing surveillance practices in the workplace. The Committee also recommends that employers must ensure a human reviews any automated decision made using workplace surveillance data that could significantly affect the rights or interests of a worker.

The protection of workplace surveillance data needs strengthening

Workplace surveillance collects personal information about employees, which can affect workers' privacy if they are unable to control who can see or use their information and how and when this data is collected, used and stored. The Committee heard that most Victorian employees do not know how data collected about them through surveillance is stored, used or disclosed, nor how long it is kept for, who has access to it and whether it may be sold to another party.

The more data an organisation holds about their employees and the longer they keep it, the greater the risk that the data may be misused or accessed inappropriately or maliciously. Data breaches can have significant negative consequences if sensitive information is exposed, especially biometric data, such as fingerprints and facial scans, because it cannot be reissued or changed once it has been compromised.

The only Australian jurisdiction that requires employers to protect workplace surveillance records is the ACT. In Victoria, the Information Privacy Principles in the *Privacy and Data Protection Act 2014* (Vic) govern how people's personal information is handled, but it only applies to the Victorian public sector, and it does not include biometric data in its definition of sensitive information. As mentioned above, the federal Privacy Act has exemptions, which results in a significant proportion of Victorian employees having no protection when it comes to the privacy of their personal information.

The European Union's General Data Protection Regulation, which is based on key principles such as fairness, transparency, purpose limitation and data minimisation, is considered best practice for protecting the privacy of personal information. The Committee recommends that new workplace surveillance legislation requires employers to inform employees of how workplace surveillance data will be secured, stored and disposed of, who collects and uses the data and for what purpose, and how long the data will be kept. Furthermore, employers must only collect biometric data for a legitimate purpose that cannot be achieved by less intrusive means and biometric data should be included in the Privacy and Data Protection Act's definition of sensitive information.

The Committee also recommends that employers give employees access to data held about them upon request, that Victoria introduce a mandatory data breach notification scheme, and that an independent workplace surveillance regulator is appointed to keep employers accountable and investigate complaints. The Victorian Government should also extend the privacy protections embedded in the Privacy and Data Protection Act to all Victorian employees, not just those in the public sector.

By implementing the recommendations in this report, and ensuring workplace surveillance is reasonable, necessary and proportionate, the Victorian Government retains employers' ability to conduct workplace surveillance, but in a way that also protects workers' rights and privacy.

Findings and recommendations

2 Workplace surveillance practices in Victoria

FINDING 1: While workplace surveillance has a long history, advances in surveillance technology and the pandemic-induced shift to remote working has made workplace surveillance easier, cheaper and more pervasive in Victorian workplaces. 26

FINDING 2: Employers are increasingly using artificial intelligence to process surveillance data and make conclusions about workers' behaviour, sentiment and performance, which could result in unfair outcomes if the decisions are based on inaccurate assumptions or interpretations. 32

FINDING 3: Employers in Victoria are seldom fully transparent about their surveillance practices so many workers are unaware of the extent of surveillance in their workplace and how their employers are using the associated data. 35

FINDING 4: Function creep, where surveillance that is deployed for a specific purpose such as safety begins to be used covertly for other reasons such as performance management, is unfair and distressing to employees and poses risks to their privacy and health and safety. 39

3 Impacts of workplace surveillance

FINDING 5: Research shows that workplace surveillance is unlikely to significantly improve workers' productivity and can produce counterproductive behaviours instead. 44

FINDING 6: Workplace surveillance that employees see as intrusive and lacking transparency reduces employees' trust in management, job satisfaction and commitment to their organisation, which can result in disengagement, poor workplace culture and increased staff turnover. 48

FINDING 7: The pressure of being constantly monitored and tracked at work leads to work intensification, where employees work harder and faster and take fewer breaks, creating occupational health and safety risks. 50

FINDING 8: Workplace surveillance that is constant, intrusive or tied to performance measures or disciplinary processes creates stress for employees resulting in poor physical and mental health and can push employees towards taking safety risks that can lead to workplace accidents and injuries. 54

FINDING 9: Workplace surveillance has the potential to impinge on the privacy of workers as well as that of their families and community members who may also be recorded by surveillance devices outside of the workplace, such as in work vehicles or in the home. 58

FINDING 10: Workplace surveillance exacerbates the power imbalance between employers and employees by giving employers greater visibility of their employees' actions and behaviours while withholding access to this surveillance data from employees. 59

FINDING 11: Workers cannot safely opt out or genuinely consent to workplace surveillance if objecting will lead to the loss of employment or possible retaliation from their employer. 59

FINDING 12: The fear of being seen to be talking with union officials or having their communications monitored has a chilling effect on workers' conversations with each other and with union officials, and this undermines collective bargaining efforts. 61

FINDING 13: Workers who are marginalised and have weaker bargaining positions, such as women, young people, migrants, members of the LGBTIQA+ community, people with disability and platform workers, are more likely to experience the harmful impacts of intense workplace surveillance. 64

4 Regulation of workplace surveillance

FINDING 14: Victoria's workplace surveillance laws are ineffective and in need of updating because they do not cover all scenarios or technologies and do not require employers to notify or consult with their employees about surveillance in the workplace. 71

FINDING 15: While workplace surveillance laws in New South Wales and the Australian Capital Territory provide workers with more protections than Victorian legislation, they should not be considered best-practice examples because they do not cover all technologies and scenarios and nor do they require workplace surveillance to be reasonable, necessary and proportionate. 75

FINDING 16: Federal laws such as the *Fair Work Act 2009* (Cth) and *Privacy Act 1988* (Cth) do not specifically refer to workplace surveillance and there are gaps in the types of records and employers they cover, which provides workers limited privacy protection. 77

FINDING 17: Australia has no obligations under international conventions to regulate or prohibit the surveillance of workers because there are no legally binding international conventions directly related to workplace surveillance. 80

FINDING 18: Best-practice regulation of workplace surveillance incorporates the principles of reasonableness, necessity, proportionality, fairness, transparency and data minimisation. 83

FINDING 19: Victoria has the power to regulate workplace surveillance under Section 27(2)(m) of the *Fair Work Act 2009* (Cth). 85

RECOMMENDATION 1: That the Victorian Government introduce new principles-based workplace surveillance legislation that is technology neutral, defines a workplace as wherever work occurs, and places a positive obligation on employers to prove through a risk assessment that any surveillance they conduct is reasonable, necessary and proportionate to achieve a stated legitimate objective. 92

RECOMMENDATION 2: That the Victorian Government include requirements for notification and disclosure in new workplace surveillance legislation that oblige employers to give 14 days' written notice to workers of workplace surveillance and that the notice specifies the methods, scope, timing and purpose of the surveillance and how the surveillance data will be used and stored. 93

RECOMMENDATION 3: That the Victorian Government include the requirement in new workplace surveillance legislation for employers to consult with employees before introducing or changing surveillance practices in the workplace. 94

RECOMMENDATION 4: That the Victorian Government require employers who conduct surveillance to have a workplace surveillance policy that is provided to all employees and reissued to employees whenever the policy is updated. 94

RECOMMENDATION 5: That the Victorian Government restrict covert workplace surveillance to cases where an employee is suspected of unlawful activity, the employer has obtained a court order to undertake the surveillance, and an independent surveillance supervisor has been appointed to the case. 94

RECOMMENDATION 6: That the Victorian Government require employers have a person with delegated authority review any automated decision made using workplace surveillance data that could significantly affect the rights, interests or employment status of a worker, including a platform worker. 97

FINDING 20: Requiring employers to disclose details and consult with workers about introducing or changing surveillance practices in the workplace would not impose a significant burden on employers and would reduce the risk of harm to workers and potential unfair dismissal or compensation claims in the future. 98

RECOMMENDATION 7: That the Victorian Government work with employer groups to provide education and support services and material to employers about any changes to workplace surveillance regulation. 99

FINDING 21: Employees' privacy is at risk from unauthorised surveillance by third parties in the workplace, which can cause psychological stress and possibly reputational damage if recordings are disseminated through social media or other media channels. 101

RECOMMENDATION 8: That the Victorian Government require employers to take all reasonable steps to prevent surveillance of an employee while at work by a party other than the employer without the employee's consent. 101

5 Surveillance data and employee privacy

FINDING 22: There is little transparency around how Victorian employers are currently using, sharing and storing workplace surveillance data. 106

FINDING 23: Employers who retain workplace surveillance data unnecessarily or do not securely store it increase the risk that employees' personal information may be misused or accessed inappropriately or maliciously. 109

FINDING 24: The *Privacy and Data Protection Act 2014* (Vic) has several gaps, which means it is ineffective at protecting all employees' personal information; for example, it only applies to Victorian public sector organisations, and it does not recognise biometric data as a form of sensitive personal information. **111**

FINDING 25: The Australian Capital Territory is the only Australian jurisdiction that regulates the handling of workplace surveillance data, making it an offence for employers to fail to protect records from misuse, loss and unauthorised access, modification or disclosure, and to fail to destroy or de-identify records that are no longer needed. **112**

FINDING 26: Exemptions for small businesses and employee records in the *Privacy Act 1988* (Cth) mean a significant amount of Victorian employees' personal information does not have privacy protection. **115**

FINDING 27: The European Union's General Data Protection Regulation that lists seven key principles for the processing of personal data and sets out individuals' data privacy rights is considered internationally as best-practice regulation for information privacy. **119**

FINDING 28: Recent changes to the *Privacy Act 1988* (Cth) do not address shortcomings in how employees' personal information is protected and, since further changes are not expected in the near future, this reinforces the need for Victoria to strengthen data protection regulation. **121**

RECOMMENDATION 9: That the Victorian Government include a requirement in new workplace surveillance legislation that employers must inform employees who is collecting workplace surveillance data, how the data is secured, stored and disposed of, who can use the data and for what purpose, and how long the data will be kept. **123**

RECOMMENDATION 10: That the Victorian Government include a provision in new workplace surveillance legislation that employers must not sell employees' personal data, or any data collected about employees through surveillance, to a third party. **123**

RECOMMENDATION 11: That the Victorian Government include a requirement in new workplace surveillance legislation that employers must ensure that any third party they contract to collect or store workplace surveillance data takes reasonable steps to protect the data and complies with the employers' workplace surveillance policy. **124**

RECOMMENDATION 12: That the Victorian Government amend the *Privacy and Data Protection Act 2014* (Vic) to introduce a new Information Privacy Principle, modelled on Australian Privacy Principle 1.2, that places a positive obligation on organisations and employers to ensure they comply with the Information Privacy Principles. **124**

RECOMMENDATION 13: That the Victorian Government include a requirement in new workplace surveillance legislation that employers, upon request by an employee, must give the employee access to workplace surveillance data generated about the employee. **125**

RECOMMENDATION 14: That the Victorian Government amend the *Privacy and Data Protection Act 2014* (Vic) to include biometric data in the definition of sensitive information. **126**

RECOMMENDATION 15: That the Victorian Government through new workplace surveillance legislation restrict employers from collecting and using employees' biometric data to circumstances where there is a legitimate purpose that cannot be achieved through less intrusive means. **127**

RECOMMENDATION 16: That the Victorian Government amend the *Privacy and Data Protection Act 2014* (Vic) to introduce a mandatory incident notification scheme that requires organisations to inform affected individuals and the Office of the Victorian Information Commissioner of a data breach. **128**

RECOMMENDATION 17: That the Victorian Government extend the privacy protections embedded in the *Privacy and Data Protection Act 2014* (Vic) to employees in all sectors by requiring employers operating in Victoria who engage in a workplace surveillance activity to comply with the Information Privacy Principles. **128**

FINDING 29: An independent regulator of workplace surveillance would keep employers accountable and give employees an avenue to address any grievances. **131**

RECOMMENDATION 18: That the Victorian Government appoint the Office of the Victorian Information Commissioner, WorkSafe Victoria or other appropriate body as a regulator and adequately resource it to oversee new workplace surveillance legislation with the power to inspect workplaces, investigate and resolve complaints, and prosecute offences. **131**

Acronyms and terms

ACT	Australian Capital Territory
AI	Artificial intelligence
Ai Group	Australian Industry Group
APPs	Australian Privacy Principles
ASU	Australian Services Union
BCA	Business Council of Australia
CBA	Commonwealth Bank of Australia
CCTV	Closed-circuit television
CPSU	Community and Public Sector Union
CWU	Communication Workers Union
DPIA	Data protection impact assessment
EU	European Union
FSU	Finance Sector Union
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HR	Human resources
ICO	Information Commissioner's Office
IEU	Independent Education Union
ILO	International Labour Organization
IPPs	Information Privacy Principles
IT	Information technology
LIV	Law Institute of Victoria
NSW	New South Wales
NT	Northern Territory
NTEU	National Tertiary Education Union
OAIC	Office of the Australian Information Commissioner
OHS	Occupational health and safety
OVIC	Office of the Victorian Information Commissioner
QLRC	Queensland Law Reform Commission
QUT	Queensland University of Technology
RFID	Radio-frequency identification
SA	South Australia
UEBA	User and entity behaviour analytics
UK	United Kingdom

UWU	United Workers Union
VFF	Victorian Farmers Federation
Victorian Chamber	Victorian Chamber of Commerce and Industry
VLRC	Victorian Law Reform Commission
VPS	Victorian public sector
VTHC	Victorian Trades Hall Council
WA	Western Australia

Figures

1 Introduction

Figure 1.1 Forms of workplace surveillance 3

Figure 1.2 Purposes of workplace surveillance 5

3 Impacts of workplace surveillance

Figure 3.1 Impact of workplace surveillance on workers 43

Tables

4 Regulation of workplace surveillance

Table 4.1 Comparison of workplace surveillance legislation in the ACT, NSW and Victoria 73

Table 4.2 Examples of workplace surveillance regulation overseas 78

Case studies

2 Workplace surveillance practices in Victoria

Case Study 2.1 '[W]orkers were made to feel shamed and distressed' 21

Case Study 2.2 'That triggered the AI to say there is actually a problem' 28

Case Study 2.3 'My state manager would routinely track field staff' 36

3 Impacts of workplace surveillance

Case Study 3.1 '[T]his is affecting their mental health in really serious ways' 53

Case Study 3.2 '[T]hat is all on camera' 55

4 Regulation of workplace surveillance

Case Study 4.1 'We introduced that policy to the staff very carefully' 81

Chapter 1
Introduction

In a modern workplace, employers are able to monitor workplace activities using a range of surveillance technologies, from conventional closed-circuit television (CCTV) cameras and phone call recordings to body-worn cameras and software that can track employees' logins, keyboard activity, tone of voice and sentiment. These tools can amass a large amount of data on employees, creating both privacy and security risks.

Employers have genuine reasons for conducting workplace surveillance such as monitoring the use of resources and property, detecting fraud and theft, improving workplace safety and recording a workplace injury or incident should one occur. At the same time, employees have a reasonable expectation of privacy in the workplace.

Workplace surveillance has become increasingly sophisticated, affordable and widespread over the past two decades, yet the last major change to Victoria's workplace surveillance laws occurred in 2006. The intervening years have seen smartphones, artificial intelligence (AI) and remote working become commonplace, and governments around Australia and the world are recognising that existing privacy and surveillance laws have not kept pace.

On 14 May 2024, the Legislative Assembly's Economy and Infrastructure Committee received terms of reference to conduct an inquiry into workplace surveillance, and specifically the extent to which surveillance data is being collected, shared, stored, disclosed, sold, disposed of and otherwise utilised in Victorian workplaces.

The detailed terms of reference also asked the Committee to consider the effectiveness of existing privacy and workplace laws to regulate workplace surveillance, the impact of workplace surveillance on workers and workplace relations, potential privacy and data security risks, and best-practice workplace surveillance and privacy laws interstate and overseas.

During the Inquiry, the Committee received evidence from unions, industry groups, legal experts, academics, individual workers and government bodies. It heard that while workplace surveillance is necessary, in some instances it can be detrimental to workers, organisational culture and workplace relations, especially when it is unreasonable or excessive. This report recognises the legitimate role of workplace surveillance in some instances but makes a series of recommendations that aim to protect workers' privacy and autonomy by modernising Victoria's workplace surveillance laws and strengthening data protections.

1.1 Workplace surveillance is more sophisticated and far-reaching now

Surveillance is the purposeful monitoring of a person, place or object to obtain information and/or influence the behaviour of the person being monitored.[1] It can be overt, if the person being monitored is aware that surveillance is happening or the surveillance device is not concealed, or covert, where the person is unaware of the monitoring or the device is concealed.[2]

In the workplace, it is common for employers to monitor workplace activities especially in larger companies and organisations. The most common methods of surveillance include CCTV cameras, monitoring of computer activities, global positioning system (GPS) location tracking and recording of telephone calls.

In its submission, the Victorian Government made a distinction between surveillance and recordkeeping in the workplace.[3] Employers are required to keep records for operational needs, compliance and external accountability. These records can include employees' payment and health information for example, and employers must protect this information in accordance with state and federal privacy laws. Workplace surveillance goes beyond recordkeeping; it involves active monitoring and recording of employees' activities and behaviours to monitor how work is performed with the aim of ensuring compliance with company policies and enhancing productivity. There is minimal regulation of data created from workplace surveillance in Victoria.

Surveillance in the workplace has a long history. It was traditionally a manual process where managers directly observed employees as they worked. American inventor and engineer Frederick Taylor's theory of scientific management in the early twentieth century further enabled this through changes to office and factory layouts to enable direct observation as part of a broader exercise to maximise efficiency and labour productivity.[4]

Since then, workplace surveillance has evolved alongside technology that allows managers to monitor multiple employees at once without being physically present. Capabilities have advanced from conventional forms of surveillance to automated software that can analyse behaviour, performance and sentiment both inside and outside the workplace. Surveillance has become more sophisticated, and employers now have greater access to employee information than ever before. These advances

---

1 Australian Law Reform Commission, *For your information: Australian privacy law and practice*, report 108, vol. 1, Australian Government, Sydney, 2008, p. 413; Kirstie Ball, *Electronic monitoring and surveillance in the workplace: literature review and policy recommendations*, Publications Office of the European Union, Luxembourg, 2021, p. 10.

2 Peter Leonard, 'Workplace surveillance and privacy', *Computers and Law: Journal for the Australian and New Zealand Societies for Computers and the Law*, vol. 93, 2021, p. 61.

3 Victorian Government, *Submission 43*, p. 3.

4 Joanna Bronowicka, et al., *'Game that you can't win'?: workplace surveillance in Germany and Poland*, European University Viadrina, Frankfurt, 2020, p. 6; United Workers Union, *Submission 25*, p. 5.

in workplace surveillance, and the broadening of its scope, have attracted renewed interest from workers, labour unions, legal experts, policymakers and the public.[5]

The following sections discuss the forms workplace surveillance can take, the reasons employers conduct it and the types of data it creates.

1.1.1 Employers can use a wide range of surveillance methods

Workplace surveillance broadly falls under five categories: optical, listening, data (computer), tracking and physical. Figure 1.1 lists the different forms of workplace surveillance that might fall under each category. See Chapter 2 for examples of surveillance occurring in Victorian workplaces that the Committee was presented with during the Inquiry.

Figure 1.1 Forms of workplace surveillance

Sources: Victorian Trades Hall Council, *Submission 28*, p. 7; Institute for Public Policy Research, *Watching me, watching you: worker surveillance in the UK after the pandemic*, report prepared by Henry Parkes, London, March 2023, p. 8.

5 Bronowicka, et al., *'Game that you can't win'?*, p. 6; Eurofound, *Employee monitoring and surveillance: the challenges of digitalisation*, Publications Office of the European Union, Luxembourg, 2020, p. 30; Oliver G. Kayas, 'Workplace surveillance: a systematic review, integrative framework, and research agenda', *Journal of Business Research*, vol. 168, 2023, p. 1, doi: 10.1016/j.busres.2023.114212; Office of the Victorian Information Commissioner, *Guiding principles for surveillance*, 2022, <https://ovic.vic.gov.au/privacy/resources-for-organisations/guiding-principles-for-surveillance> accessed 13 May 2024; Centre for Decent Work and Industry, QUT, *Submission 13*, p. 1; Victorian Government, *Submission 43*, p. 16.

As the figure shows, employers can use a wide range of surveillance techniques that are often unremarkable but can be pervasive, creating an environment where workers could be watched constantly at work and even at home with the rise of remote working. Workers' movements can be tracked through swipe cards, body-worn radio-frequency identification (RFID) tags, mobile phones, fingerprints or handheld barcode scanners, and their activities recorded through computer and phone logging, eye-tracking software (to show whether or where they are looking at the screen), mobile phone application use and rostering software. These techniques may be used on an ongoing basis, such as keystroke logging, or randomly, such as screenshots or webcam photos. Often, employees may not even know they are being monitored.[6]

The types of surveillance techniques and how they are used vary by industry. Some small businesses will rarely undertake surveillance whereas larger organisations especially in the logistics, warehousing and financial industries employ multiple methods on a constant basis. In some instances, these techniques may be used to check employees' physical presence, facial expressions, frequency of speech and conversation content. AI can then be used to analyse the data and make decisions about employees' mood, attitude and performance.[7]

Wearable devices, such as smartwatches, body cameras and smart clothing, can also feed data into software that analyses production and work processes. These devices can have motion sensors, location sensors, microphones and other technologies, and because the devices are always on, they can track employees' movements and location throughout the workday.[8] Other surveillance tools can monitor individual workers' production rates, compare the rates to set targets or those of other workers, and display the results on screens in the workplace.[9]

Another technology employed in workplace surveillance is biometrics. Biometric surveillance involves the collection or recording of biological or physical characteristics to identify an individual. Biometric data can include fingerprints, iris scans and retinal scans, as well as information derived from facial, voice or gait recognition technologies, cheek swabs or blood samples. Biometric surveillance can also include the use of alert

---

6 United Workers Union, *Submission 25*, p. 6; Bronowicka, et al., *'Game that you can't win'?*, p. 6; Roger Clarke, 'Responsible application of artificial intelligence to surveillance: what prospects?', *Information Polity*, vol. 27, no. 2, 2022, p. 176; Wendi S. Lazar and Cody Yorke, 'Watched while working: use of monitoring and AI in the workplace increases', *Reuters*, 26 April 2023, <https://www.reuters.com/legal/legalindustry/watched-while-working-use-monitoring-ai-workplace-increases-2023-04-25> accessed 16 May 2024.

7 Bronowicka, et al., *'Game that you can't win'?*, p. 7; Wilneida Negrón and Aiha Nguyen, 'The long shadow of workplace surveillance', *Stanford Social Innovation Review*, 6 September 2023, <https://ssir.org/articles/entry/the_long_shadow_of_workplace_surveillance> accessed 17 July 2024.

8 Eurofound, *Employee monitoring and surveillance*, p. 5; Thomas Kalischko and René Riedl, 'Electronic performance monitoring in the digital workplace: conceptualization, review of effects and moderators, and future research opportunities', *Frontiers in Psychology*, vol. 12, 2021, p. 2, doi: 10.3389/fpsyg.2021.633031

9 Dan Nahum and Jim Stanford, Centre for Future Work, Australia Institute, *Technology, standards and democracy*, submission to NSW Legislative Council Select Committee on the Impact of technological and other change on the future of work and workers in New South Wales, 2020, p. 8; Laundry Association Australia, *Submission 12*, p. 2.

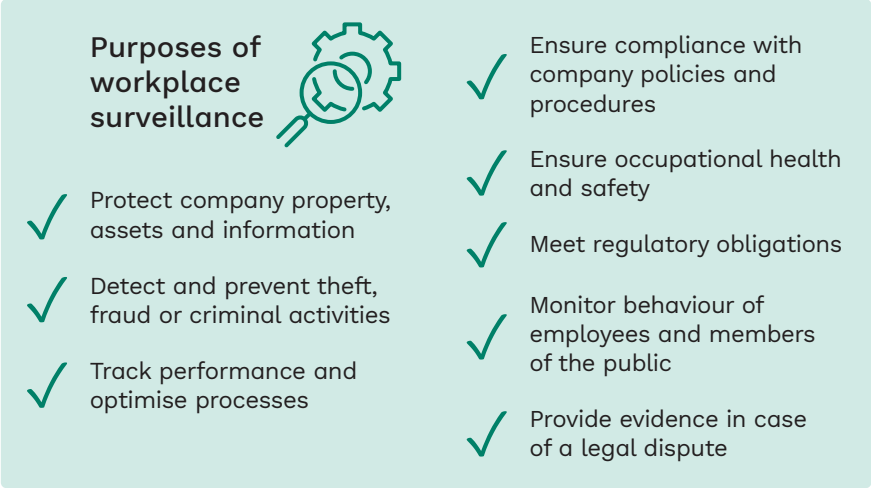
monitors in vehicles or heavy machinery to monitor driver fatigue and fitness trackers to encourage employees to stay fitter and healthier.[10]

Last, it is important to highlight that not all surveillance is conducted using technology. Managers can still use direct observation to monitor and influence workers' behaviour.[11]

1.1.2 There are legitimate reasons for workplace surveillance

Workplace surveillance is used for a variety of legitimate purposes and is typically considered a standard element in the workplace.[12] Figure 1.2 lists reasons why employers may use workplace surveillance.

Figure 1.2 Purposes of workplace surveillance



Sources: Leonard, *Workplace surveillance and privacy*, p. 60; Eurofound, *Employee monitoring and surveillance*, p. 3, Information Commissioner's Office UK, *Employment practices and data protection*; Bronowicka, et al., *'Game that you can't win'?*, p. 8; Victorian Trades Hall Council, *Submission 28*, p. 10.

Surveillance is necessary in highly regulated sectors such as banking, casinos and food manufacturing to detect fraudulent behaviour and ensure processes are followed to protect the public. Other workplaces have to ensure restricted access to certain areas to protect controlled substances or information.[13]

Surveillance can help mitigate data security and safety risks as work and the economy become more digitised and data breaches caused by careless or rogue employees

---

10 Information Commissioner's Office UK, *Employment practices and data protection: monitoring workers*, October 2023, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers> accessed 14 May 2024; Leonard, 'Workplace surveillance and privacy', p. 67; Peter Holland and Tse Leng Tham, 'Workplace biometrics: protecting employee privacy one fingerprint at a time', *Economic and Industrial Democracy*, vol. 43, no. 2, 2022, p. 502; Eurofound, *Employee monitoring and surveillance*, p. 32.

11 Lauren Kelly, Research and Policy Officer, United Workers Union, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, pp. 40–41.

12 Kayas, 'Workplace surveillance', p. 1.

13 Ramsay Health Care Australia, *Submission 15*, p. 1; United Workers Union, *Submission 25*, p. 6; Institute for Public Policy Research, *Watching me, watching you: worker surveillance in the UK after the pandemic*, report prepared by Henry Parkes, London, 2023, p. 8.

create new vulnerabilities for employers. Employers can also use surveillance to avoid work injuries and meet their obligations under occupational health and safety laws.[14] For example, CCTV and body-worn cameras have been used to reduce harm to healthcare, transport and retail workers when they interact with members of the public who may be violent or aggressive.[15]

Employer and industry groups reiterated these reasons to the Committee to explain employers' use of workplace surveillance. They mentioned its usefulness for ensuring the health and safety of workers and noted that the state's workplace health and safety regulator, WorkSafe Victoria, sees automated warning devices, CCTV and GPS tracking systems as ways to address occupational health and safety risks.[16] Similarly, they highlighted that surveillance can be used to train workers and provide feedback, accurately record overtime hours so that employees are correctly paid, and deter and help investigate cases of discrimination and sexual harassment, which employers have a positive duty to eliminate under occupational health and safety laws.[17]

Employers also use workplace surveillance to improve productivity and manage resources efficiently.[18] For example, the Laundry Association of Australia, which represents commercial, industrial and public sector laundry operators across Australia, explained that laundry operators use workflow management control software to monitor, identify and sort linen as well as process line workers' rate of feeding individual textile items into equipment such as folding machines. Operators have found that this software has improved productivity by 5–10%.[19]

Despite having legitimate reasons to conduct workplace surveillance, other possible motivations for employers might include encouraging greater effort from employees during work hours, observing workers' interactions with each other, predicting workers' future behaviour and identifying areas where jobs could be replaced with automation.[20]

The Committee also heard that some employers conduct surveillance simply because they have the capability and there are no legal constraints to limit them.[21] As

---

14 Murray Brown and Normann Witzleb, 'Big brother at work: workplace surveillance and employee privacy in Australia', *Australian Journal of Labour Law*, vol. 34, no. 3, 2021, p. 4; Office of the Victorian Information Commissioner, *Submission 39*, p. 8; Victorian Government, *Submission 43*, p. 12.

15 Centre for Decent Work and Industry, *Submission 13*, p. 9; Australian Nursing and Midwifery Federation, Victorian Branch, *Submission 38*, p. 4.

16 Master Electricians Australia, *Submission 11*, pp. 3–4; Ramsay Health Care Australia, *Submission 15*, p. 1; Victorian Automobile Chamber of Commerce, *Submission 26*, p. 7; Australian Industry Group, *Submission 40*, pp. 5–7.

17 Laundry Association Australia, *Submission 12*, p. 3; Victorian Automobile Chamber of Commerce, *Submission 26*, p. 7; Australian Industry Group, *Submission 40*, p. 8; Commonwealth Bank of Australia, *Submission 44*, p. 1; Kat Eather, General Counsel, Business Council of Australia, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, pp. 18–19; Georgia Holmes, Policy and Communications Advisor, Master Electricians Australia, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 26.

18 Victorian Automobile Chamber of Commerce, *Submission 26*, p. 7; Victorian Government, *Submission 43*, p. 12.

19 Laundry Association Australia, *Submission 12*, p. 2.

20 Victorian Government, *Submission 43*, p. 13.

21 Dr Dale Tweedie, Senior Lecturer, Department of Accounting and Corporate Governance, Macquarie University, public hearing, 26 September 2024, *Transcript of evidence*, p. 12.

Professor of Human Resource Management at Swinburne University of Technology's School of Business, Law and Entrepreneurship, Peter Holland, told the Committee:

> I have taught postgraduate at both Swinburne and when I was at Monash, and I ask students, postgrads who are HR [human resources] managers, 'Do you monitor and surveil your workforce?' And they say yes, and I say why, and they say, 'Because we can'—because there is no legal regulation to stop them.[22]

Section 1.2 outlines the existing state and federal regulation around workplace surveillance.

Employees recognise that in certain situations workplace surveillance is good practice, for example, when it protects the safety of staff, identifies maintenance issues, enhances training or exposes harmful behaviours. However, they can see it as problematic if it gathers information beyond the working environment or unrelated to work performance, compromises work practices or reduces autonomy and trust.[23]

1.1.3 Workplace surveillance can collect a vast amount of data

Digital surveillance technologies can capture a large amount of data across a wide range of domains. In the workplace, they can record shift start and end times, time spent on websites or specific programs, email and instant messaging content, keyboard activity, screenshots, time spent at the computer, location, surrounding footage and/or sound, break times and task rates.[24] Some technologies can collect sensitive information such as financial data, medical data and biometric data, for example tone of voice, heart rate, step count and body temperature.[25]

The different types of data collected by workplace surveillance can cover many aspects of workers' lives including location, movement, task performance, physiology, thoughts, feelings, professional profile and reputation. One example is digital platform work where data on gig economy workers' performance, behaviour and location is captured alongside customer feedback and used to decide future work offers and rewards using algorithms.[26] Data collected through workplace surveillance can be analysed using AI to build behaviour patterns and profiles notifying managers if any changes are detected in workers' behaviour.[27] In these situations, surveillance can go beyond what a worker is doing at any given moment to monitoring their level of engagement and predicting future behaviour such as seeking a raise or searching for another job.[28]

---

22 Professor Peter Holland and Dr Jacqueline Meredith, Swinburne University of Technology, *Submission 22*, p. 2.

23 Kayas, 'Workplace surveillance', p. 1; United Workers Union, *Submission 25*, p. 6; Victorian Trades Hall Council, *Submission 28*, p. 9.

24 Victorian Government, *Submission 43*, p. 4; Bronowicka, et al., *'Game that you can't win'?*, p. 4.

25 Bronowicka, et al., *'Game that you can't win'?*, p. 4; Colleen Chen and John Howe, *Worker data right: the digital right of entry*, policy brief, no. 5, Centre for Employment and Labour Relations Law, University of Melbourne, 2022, p. 3.

26 Ball, *Electronic monitoring and surveillance in the workplace*, p. 6.

27 Ibid.; Bronowicka, et al., *'Game that you can't win'?*, p. 7.

28 Kate Morgan and Delaney Nolan, 'How worker surveillance is backfiring on employers', *BBC*, 30 January 2023, <https://www.bbc.com/worklife/article/20230127-how-worker-surveillance-is-backfiring-on-employers> accessed 15 May 2024.

1.1.4 Workplace surveillance laws in Australia are inconsistent

There is little consistency between workplace surveillance laws across Australia's jurisdictions, as discussed in this section. New South Wales (NSW) and the Australian Capital Territory (ACT) have dedicated legislation whereas Victoria's laws are integrated into general surveillance device laws. The other states and territory do not have specific workplace surveillance legislation, and there are no federal laws either. The effectiveness of existing laws is covered in Chapter 3.

Victoria's laws are embedded in general surveillance legislation

Victoria does not have dedicated workplace surveillance laws. Instead, the regulation of workplace surveillance is embedded in the *Surveillance Devices Act 1999* (Vic), which was amended in 2006 to incorporate workplace surveillance through prohibiting the use of surveillance devices (specifically cameras and listening devices) in workplace toilets, bathrooms, change rooms and lactation rooms.[29]

The Surveillance Devices Act allows surveillance of private activities and conversations if the people being recorded have given express or implied consent.[30] The definition of private activities and conversations excludes those where the parties would reasonably expect they could be watched or overheard, making it unlikely that activities and conversations in business settings would be considered private.[31] The Act allows for GPS tracking if the person being tracked gives express or implied consent. Data surveillance is only referred to in terms of its use by law enforcement officers; the Act is silent on the use of data surveillance by employers or members of the public.[32]

Section 13 of the *Charter of Human Rights and Responsibilities Act 2006* (Vic) gives every Victorian the right to not have their privacy, family life, home or correspondence, such as mail or email, interfered with.[33] The Charter applies to public authorities in Victoria. Similarly, privacy rights under the *Privacy and Data Protection Act 2014* (Vic) protect the personal information held by Victorian public sector (VPS) organisations, which includes the data of VPS employees.

The Privacy and Data Protection Act aims to balance the public interests of the free flow of information with protecting the privacy of personal information. It has 10 Information Privacy Principles (IPPs) that cover the collection, use, disclosure and storage of personal information as well as individuals' rights to access and amend their personal information.[34]

---

29 *Surveillance Devices Act 1999* (Vic) s 9B.

30 *Surveillance Devices Act 1999* (Vic) ss 6(1), 7(1).

31 Victorian Law Reform Commission, *Workplace privacy: final report*, Melbourne, 2005, p. 21; Law Institute of Victoria, *Submission 37*, p. 3.

32 *Surveillance Devices Act 1999* (Vic) ss 8, 9.

33 *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13.

34 Office of the Victorian Information Commissioner, *Information privacy principles: full text*, 2021, <https://ovic.vic.gov.au/privacy/resources-for-organisations/information-privacy-principles-full-text> accessed 22 November 2024.

The public sector organisations captured in the Privacy and Data Protection Act include Victorian Government departments and agencies, local government, Victoria Police, ministers and other bodies such as public hospitals and public schools. The privacy of personal information held by public hospitals, health service providers and other organisations that handle health information is regulated by the *Health Records Act 2001* (Vic). These entities are also required to take reasonable steps to protect their employees' personal information.[35]

NSW has dedicated workplace surveillance laws

There are two acts in NSW that deal with workplace surveillance: the *Workplace Surveillance Act 2005* (NSW) and the *Surveillance Devices Act 2007* (NSW). The Workplace Surveillance Act permits the monitoring of employees in the workplace—which can include the home if a person works from there—provided they have been formally notified at least 14 days prior, signage is placed in relevant areas and the employer has a monitoring policy. The notification must include how the surveillance will be carried out, when it will begin and whether it will be intermittent or continuous. It covers surveillance by camera, computer and tracking devices; surveillance by a listening device is regulated by the Surveillance Devices Act. Surveillance of an employee must not occur in a change room, toilet facility or bathroom.[36]

ACT's workplace surveillance laws are the most comprehensive

The *Workplace Privacy Act 2011* (ACT) provides similar protections to the NSW Workplace Surveillance Act regarding the types of surveillance that can be carried out and the required notice; however, it also requires the employer to inform employees of the purpose for which the surveillance may be used and disclosed, and to consult with employees about the proposed method before the surveillance is introduced. In addition to toilets, bathrooms and change rooms, the ACT also prohibits surveillance devices in parent rooms, prayer rooms, sick bays and first aid rooms. Employers who do not take reasonable steps to protect surveillance records from misuse, unauthorised access, disclosure or loss, and who fail to destroy or de-identify records they no longer need, are deemed to have committed an offence.[37]

WA, SA and NT have general surveillance laws

Surveillance of private activities and conversations in Western Australia (WA), South Australia (SA) and the Northern Territory (NT) are covered by general surveillance laws. These laws deal with optical, tracking and listening surveillance and—except for WA—also with data surveillance. The *Surveillance Devices Act 1998* (WA), *Surveillance Devices Act 2016* (SA) and *Surveillance Devices Act 2007* (NT) allow surveillance if those being monitored have given express or implied consent.

---

35 Office of the Victorian Information Commissioner, *Your privacy rights*, 2020, <https://ovic.vic.gov.au/privacy/for-the-public/your-privacy-rights> accessed 22 November 2024.

36 *Workplace Surveillance Act 2005* (NSW) ss 10–15.

37 *Workplace Privacy Act 2011* (ACT) ss 13, 41, 44.

Queensland's and Tasmania's surveillance laws have recently been reviewed

Surveillance of employees in both Queensland and Tasmania is not specifically regulated. Furthermore, regulation of general surveillance is limited to listening devices as set out in the *Invasion of Privacy Act 1971* (Qld) and the *Listening Devices Act 1991* (Tas). The rules around private conversations and consent resemble those in WA, SA and NT.

Queensland is considering strengthening laws around surveillance. In 2020, the Queensland Law Reform Commission (QLRC) published its review of Queensland's laws relating to civil surveillance with a view to recommending whether legislation should be introduced to protect individuals' privacy around devices such as CCTV, tracking devices and drones. It recommended repealing the Invasion of Privacy Act and replacing it with new legislation that provides more comprehensive protections. The proposed reforms would apply to surveillance devices in both civil and workplace environments. The Queensland Government is currently running public consultations on how to implement the recommendations in the QLRC report.[38]

The Tasmania Law Reform Institute also conducted a recent review of the privacy laws in Tasmania. Its report, published in May 2024, concluded that existing state laws were inadequate to protect Tasmanians' privacy given technological advances and community expectations. It recommended reforms to enhance privacy protections and increase clarity around privacy obligations.[39]

Commonwealth laws do not directly regulate workplace surveillance

The *Privacy Act 1988* (Cth) makes no specific reference to surveillance in the workplace. It does, however, cover the collection, storage, use and disclosure of personal information found in employee records for current or past employees of:

- Australian Government agencies
- businesses with an annual turnover of $3 million or more
- all private health service providers.

These entities must apply the Australian Privacy Principles (APPs) to handling employee records, in addition to the handling of other people's personal information such as consumers. The APPs, which are outlined in the Privacy Act, 'set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information.'[40] Under the APPs, employers must ensure that any surveillance is reasonable and necessary, a privacy policy is in place, consent is obtained before collecting employees' personal information (including via surveillance) and that the collected data is accurate, current and stored securely.

---

38 Department of Justice and Attorney-General, *Civil surveillance reforms*, Queensland Government, Brisbane, 2023, pp. 3–4.

39 Tasmania Law Reform Institute, *Review of privacy laws in Tasmania*, final report, no. 33, Hobart, May 2024, p. xi.

40 Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, Australian Government, Sydney, 2022, p. 3.

The handling of private sector employee records is exempt from the Privacy Act.[41] In addition, many employers are not covered by the Privacy Act whatsoever because they are small businesses and do not meet the turnover threshold; according to the Australian Bureau of Statistics, 92% of Australian businesses had an annual turnover of less than $2 million in 2022–23.[42] However, workplace laws regarding information held by employers still apply, and current and former employees can request access to their records under these laws. The Fair Work Ombudsman provides guidance to employers and managers about their obligations in this space.[43]

The scope of which entities are captured by the Privacy Act could change with future privacy reforms proposed by the Attorney-General's Department, which completed a three-year review of the Privacy Act in 2022. It found there was uncertainty about what information should be protected under the Act as well as a need for more protections for personal information, more flexibility so the Act can respond to a wider range of circumstances, and stronger enforcement of privacy obligations.[44]

In response, the Australian Government aimed to introduce legislation reforming the Privacy Act focusing on expanding the scope and application of the Act, strengthening protections and enforcement, giving people more transparency over the information entities hold on them, and providing greater clarity on entities' privacy obligations.[45] While these reforms would not specifically regulate workplace surveillance, it was expected that employers' obligations around their employees' personal information would be extended under the Act.

The first tranche of reforms to the Privacy Act was introduced into Parliament in September 2024 and most of the amendments came into effect in December 2024. The key reforms include creating a statutory tort for serious invasions of privacy, establishing a Children's Online Privacy Code, requiring greater transparency around automated decision-making reached using individuals' personal information, and introducing criminal offences for doxxing (when data is exposed in a menacing or harassing way). The statutory tort will come into effect by 11 June 2025 and the transparency of automated decisions in December 2026. This tranche of reforms will not substantially change the regulation of workplace surveillance or its associated data, and the proposed removal of the small business exemption was not included. It is not clear when the second tranche of reforms will be introduced but it is unlikely to occur before the 2025 federal election.[46]

---

41 Office of the Australian Information Commissioner, *Employment*, (n.d.), <https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/employment> accessed 22 November 2024.

42 Australian Bureau of Statistics, *Counts of Australian businesses, including entries and exits*, 2023, <https://www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/jul2019-jun2023> accessed 22 November 2024.

43 Fair Work Ombudsman, *Workplace privacy best practice guide*, Australian Government, 2023.

44 Attorney-General's Department, *Privacy Act review: report on a page*, factsheet, Australian Government, Canberra, February 2023, p. 1.

45 Australian Government, *Government response: Privacy Act review report*, Canberra, 2023, pp. 2–3.

46 Geoff McGrath, et al., *Australia's first tranche of privacy reforms: a deep dive and why they matter*, Ashurst, 2024, <https://www.ashurst.com/en/insights/australias-first-tranche-of-privacy-reforms-a-deep-dive-and-why-they-matter> accessed 23 January 2025; Owen Griffiths and David McGovern, *Privacy and Other Legislation Amendment Bill 2024*, bills digest, no. 16, 2024–25, Parliament of Australia Library, November 2024, p. 1.

Other relevant federal laws include the *Telecommunications (Interception and Access) Act 1979* (Cth), which prohibits the live interception of private communications such as phone calls and access to stored communications such as emails, SMS and voicemails without the knowledge of those involved in the communication or without a warrant.[47] Employers need to notify employees that their communications are being listened to or recorded, and any surveillance would need to be conducted in accordance with the Privacy Act.[48] A 2020 review of the legal framework governing the National Intelligence Community recommended the Telecommunications (Interception and Access) Act be repealed and replaced with a new act that takes into account electronic surveillance and modern technologies such as AI. In its response, the Australian Government supported holistic reform of the legislative framework around electronic surveillance, and it is currently consulting with stakeholders while developing draft legislation.[49]

The *Fair Work Act 2009* (Cth), which protects workplace rights, does not refer to workplace surveillance. While it protects employees from discrimination based on personal attributes, which could be ascertained from surveillance data, there are no provisions to protect the privacy of workers in terms of the information collected through surveillance.[50]

1.1.5 There is growing interest in the legal frameworks around workplace surveillance

Recent international scholarship has scoped current workplace surveillance practices and reviewed published research in the field. For example, European approaches to regulating workplace surveillance were mapped out in a 2020 report alongside an overview of new forms of employee monitoring and a review of research on the impacts of surveillance on job quality. It found that the implementation of legislative reform has modernised data protection in the European Union and enhanced individuals' rights and protections regarding their personal information, including in the workplace. However, the report notes that surveillance technologies are continuously progressing and that countries need to be on guard to ensure workers' rights remain protected.[51]

A 2023 systematic review of the international literature found the topic of workplace surveillance has been approached from a wide range of disciplines, although most research has focused on ethics, organisational psychology, economics and human resource management. Published research shows workplace surveillance usually

---

47 Leonard, 'Workplace surveillance and privacy', p. 69.

48 John Wilson and Kieran Pender, 'The rights and wrongs of workplace surveillance', *Ethos: Law Society of the ACT Journal*, no. 267, 2023, pp. 24–25; Jack de Flamingh and Phillip Magness, 'The limitations of a modern day bag search', *Law Society Journal*, no. 48, September 2018, p. 77.

49 Centre for Decent Work and Industry, *Submission 13*, p. 12; Attorney-General's Department, *Commonwealth Government response to the comprehensive review of the legal framework of the national intelligence community*, Australian Government, Canberra, 2020, p. 23; Attorney-General's Department, *Reform of Australia's electronic surveillance framework*, 2020, <https://www.ag.gov.au/crime/telecommunications-interception-and-surveillance/reform-australias-electronic-surveillance-framework> accessed 22 November 2024.

50 *Fair Work Act 2009* (Cth) s 351.

51 Eurofound, *Employee monitoring and surveillance*, pp. 4, 43.

stems from motives of performance and control and has both positive and negative outcomes. The review concluded that more research is needed that considers the different national contexts of workplace surveillance, a broader range of organisations and sectors, and workers' personal experiences.[52]

Another report in 2021 re-evaluated research on workplace surveillance in light of modern workplace practices and emerging technologies. It considered the psychological responses of monitoring and new methods of people analytics. It found that employees resist surveillance in multiple ways, monitoring can have a negative impact on workplace relationships, employees should have greater say in surveillance practices, and privacy issues are becoming more important as surveillance increasingly focuses on the body and behaviours and extends into non-work time.[53]

In addition to literature reviews, several inquiries in Australia and abroad have touched on workplace surveillance in recent years. These are described below.

Inquiry into the digital transformation of workplaces

The Australian House of Representatives Standing Committee on Employment, Education and Training recently completed an inquiry into the digital transformation of workplaces. One of the terms of reference asked that Committee to examine the risks, opportunities and consequences of the advances and uptake of automated decision-making and machine learning techniques in the workplace on employee monitoring and surveillance, among other aspects of work.[54]

In its report tabled in February 2025, the Standing Committee found significant gaps in how the protection of workers' data is regulated and that excessive workplace monitoring and surveillance has a negative impact on workers' health and safety. It recommended that the Fair Work Act and Privacy Act be reviewed to:

- ban disclosure of workers' data to technology developers and the sale of workers' data to third parties
- require meaningful consultation and transparency with workers about the use of surveillance measures and data used by AI systems in the workplace
- empower the Fair Work Commission to investigate and resolve complaints relating to breaches of workers' privacy.[55]

---

52 Kayas, 'Workplace surveillance', pp. 4, 13–14.

53 Ball, *Electronic monitoring and surveillance in the workplace*, p. 79.

54 Parliament of Australia, House of Representatives Standing Committee on Employment, Education and Training, *Terms of reference, Inquiry into the digital transformation of workplaces*, 9 April 2024, <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Employment_Education_and_Training/DigitalTransformation/Terms_of_Reference> accessed 22 November 2024.

55 Parliament of Australia, House of Representatives Standing Committee on Employment, Education and Training, *The future of work: Inquiry into the digital transformation of workplaces*, February 2025, pp. 56–58.

It also recommended that the Australian Government 'work with states and territories to develop greater consistency and better protections against excessive and unreasonable surveillance in the workplace.'[56]

Inquiry into the impact of technological and other change on the future of work and workers in NSW

In 2022, a Select Committee of the NSW Legislative Council tabled its second report on the impact of technological and other change on the future of work and workers in NSW. This report focused specifically on workplace surveillance and automation whereas its first report focused on the gig economy. The Committee was asked to consider whether workplace surveillance laws and protections are fit for purpose in the twenty-first century.

It found that greater government action is needed to better manage how surveillance technologies are used in the workplace. It recommended that the Workplace Surveillance Act be amended to take into account new and emerging technologies and the changing nature of work.[57] In its response, the NSW Government acknowledged the issues raised by the Committee but stated that its departments regularly consider the need to modernise legislation to account for new technological advances and that 'no changes to relevant legislation are planned at this time.'[58]

United Kingdom inquiry into human rights at work

In 2023, the United Kingdom Parliament's Joint Committee on Human Rights began an inquiry into human rights at work looking at the extent to which human rights are protected and respected in the workplace. Surveillance at work and the right to privacy formed part of the terms of reference and the Committee considered if the current legal framework is adequate to protect workers' rights to private and family life and freedom from discrimination.[59] The Committee held three public hearings between October 2023 and January 2024 but did not table its report before the parliamentary term expired. The inquiry has since lapsed.

Victorian Law Reform Commission's inquiry into workplace privacy

The Victorian Government commissioned an inquiry into workplace privacy and surveillance more than two decades ago. In 2002, the Victorian Attorney-General asked the Victorian Law Reform Commission (VLRC) to inquire into the need for

---

56 Ibid., p. 58.

57 Parliament of New South Wales, Legislative Council Select Committee on the Impact of Technological and Other Change on the Future of Work and Workers in New South Wales, *Impact of technological and other change on the future of work and workers in New South Wales: final report—workplace surveillance and automation*, November 2022, pp. 23–25.

58 Government of New South Wales, *Response to the Parliament of New South Wales, Legislative Council Select Committee on the impact of technological and other change on the future of work and workers in New South Wales, report no. 2—workplace surveillance and automation*, 2023, p. 1.

59 UK Parliament, *Inquiry launched into human rights at work*, 2023, <https://committees.parliament.uk/committee/93/human-rights-joint-committee/news/186147/inquiry-launched-into-human-rights-at-work> accessed 17 May 2024.

legislative reforms to protect workers' privacy in view of the widespread use of workplace surveillance and other technologies. In its 2005 report, the VLRC found that technological change in the workplace gave employers unprecedented access to employees' lives and that Victoria's Surveillance Devices Act as it was then, did not adequately protect workers' privacy.[60]

The VLRC recommended that the Government introduce comprehensive workplace privacy laws that would balance employee rights with employer interests. The proposed legislation would generally prohibit surveillance that was not legitimate, necessary and proportionate and would require employers to inform and consult with employees about new workplace surveillance activities. It also recommended prohibiting surveillance in private areas such as bathrooms and toilets, and implementing strict guidelines on the storage, access and retention of surveillance data.[61] While legislation was introduced to prohibit workplace surveillance in private areas in 2006, ultimately no further action was taken on the VLRC's other recommendations by successive governments.[62]

1.2 Scope of the Inquiry

The terms of reference for this Inquiry required the Committee to examine workplace surveillance along five broad themes:

- current workplace surveillance and associated data handling practices in Victoria
- regulation of workplace surveillance—including the effectiveness of current privacy and workplace laws, how Victorian laws interact with federal laws, and Australia's obligations under international law
- potential privacy and data security risks posed by workplace surveillance on Victorian individuals, workers, businesses and communities
- the impact of workplace surveillance on workers, their families and workplace relations
- best-practice workplace surveillance and privacy laws interstate and overseas.

It became clear in the evidence received that the Committee was considering two processes that while interrelated, deal with separate issues that require separate responses; these were:

1. the act of workplace surveillance
2. the handling of the data generated through workplace surveillance.

For this reason, this report first considers workplace surveillance and its regulation before moving on to how the associated data is handled and regulated.

---

60 Victorian Law Reform Commission, *Workplace privacy*, pp. 17, 20.

61 Ibid., p. 45; Brown and Witzleb, 'Big brother at work', pp. 17–20; Victorian Government, *Submission 43*, p. 21.

62 Brown and Witzleb, 'Big brother at work', p. 21.

1.3 Inquiry process

The Committee called for submissions to this Inquiry in June 2024 by writing directly to over 140 stakeholders and advertising on LinkedIn, X, YouTube, Facebook and Instagram. The invited stakeholders included legal experts, research institutes, Victorian and Australian government bodies, unions, employer groups, privacy organisations, information technology companies and leading businesses operating in Australia.

The Committee received 44 submissions, which are listed in Appendix A. Most of these submissions were from unions followed by industry groups, individuals and academics. Several unions surveyed their members to collect quantitative and qualitative data to inform their submissions. Many union submissions also provided a range of case studies to illustrate the types of workplace surveillance employers undertake and the impacts of this surveillance on workers.

The Committee would like to note employers' lack of engagement with the Inquiry, despite the Committee's active efforts to gain their input. Only one employer, Ramsay Health Care Australia, responded to the initial call and made a submission. Other major businesses such as Amazon, Australia Post, Coles Group, DoorDash, Optus, Qantas, Telstra, Uber, Virgin Australia, Woolworths Group and the big four banks did not respond to the call for submissions and also declined a subsequent invitation to appear before the Committee at a public hearing.

The Commonwealth Bank of Australia was the only business that agreed to respond to questions in writing in place of appearing at a hearing, and the Committee accepted its responses as a submission. The Australian Retailers Association, which represents Coles Group and Woolworths Group, agreed to attend a hearing; however, it withdrew its participation shortly before its scheduled appearance, then did not respond to subsequent invitations.

The Committee held four days of public hearings from September to November 2024. Two days of hearings were held in Melbourne and two were held online over Zoom. Appendix A lists the witnesses who gave evidence at the public hearings. The public hearings were publicised on the Parliament of Victoria's website and social media feeds. All the public hearings were broadcast live on the Parliament of Victoria's website.

1.4 Report outline

This report consists of six chapters:

- This chapter, Chapter 1, introduces the Inquiry by outlining the Inquiry's context, scope and process.
- Chapter 2 discusses current workplace surveillance practices in Victoria, the role of artificial intelligence in workplace surveillance, and the extent to which employers inform their employees of the surveillance they conduct.

- Chapter 3 considers the impact workplace surveillance has on workers, organisations and workplace relations.
- Chapter 4 explores the effectiveness of current Victorian workplace surveillance laws and how these laws can be modernised.
- Chapter 5 considers how workplace surveillance data is handled in Victoria, the effectiveness of current information privacy laws, and how data protection can be strengthened.
- Chapter 6 provides a short conclusion to the report.

Chapter 2
Workplace surveillance practices in Victoria

With advances in technology and the growth of remote working, workplace surveillance is becoming more widespread, especially in larger businesses and organisations. This chapter looks at current workplace surveillance practices reported in Victoria, before exploring how changes to workplaces over the past two decades have led to present circumstances. It then considers the growing role of artificial intelligence (AI) in workplace surveillance and the implications of this development. Last, it explores the extent to which employers inform their employees of the workplace surveillance they conduct.

2.1 Workplace surveillance is growing in Victoria

Work is increasingly performed using devices such as computers, GPS (Global Positioning System) trackers, mobile phones and handheld scanners. These devices can continuously gather data on work processes and workers' activities and performance, which companies can then interpret to monitor and manage their workforce.[1] This section provides examples of the types of surveillance that Victorian workers report are operating in their workplaces. This is followed by an examination of how workplaces and workplace surveillance have changed over the past two decades.

2.1.1 Victorian employers use a wide range of surveillance practices

When asked if their workplace uses surveillance to monitor their work, 61% of respondents to a Victorian Trades Hall Council (VTHC) survey said yes, 18% said no and 21% were unsure.[2] The VTHC, which is the peak body for 40 affiliated Victorian unions, surveyed over 370 workers for its submission to this Inquiry. It found that the most common forms of surveillance reported by respondents were video surveillance, email monitoring, social media monitoring, surveillance of break rooms and audio surveillance. Less common forms were keystroke monitoring, wearable devices, always active webcams and remote screenshotting of computer screens.[3]

The National Tertiary Education Union (NTEU), which represents all higher education and university employees in Australia, also surveyed its members for the Inquiry, and of the 455 respondents, 53% reported being surveilled at their workplace, 35% were

1 Brishen Rogers, 'The law and political economy of workplace technological change', *Harvard Civil Rights—Civil Liberties Law Review*, vol. 55, 2020, p. 532.

2 Victorian Trades Hall Council, *Submission 28*, p. 14.

3 Ibid., p. 15.

unsure and 12% said they were not surveilled. The most common forms of surveillance reported were video and the monitoring of computer usage, internet and emails.[4] Other respondents spoke of heat tracking in rooms, number plate recognition devices at point of entry and the replacement of physical keys with RFID (radio-frequency identification) cards tied to mobile devices to access buildings.[5] Several respondents pointed out employers' use of Microsoft Teams, which shows real-time computer activity and provides usage analytics to managers, as well as it being a vehicle for required group chats and phone check-ins throughout the day.[6]

The Committee also heard examples of employers monitoring workers' social media to see how workers' online activity reflected on the company they work for, and on days when workers called in sick, employers are using it to identify inconsistencies with being ill through geotags or other social media data.[7] Finance sector workers mentioned how all their communications throughout the workday are recorded, including in person and via telephone, email, instant messaging, Zoom, Microsoft Teams and social media.[8] Transport workers spoke of cameras inside their vehicles that shine infrared beams onto their eyes and faces for up to 12 consecutive hours to identify distraction or fatigue.[9] Other unions reported workers' biometric data, such as retina, finger, hand and facial features, is being collected as a condition of work and that some employers have used undercover representatives or private investigators to monitor their staff.[10]

The Australian Manufacturing Workers' Union, which represents workers in all areas of manufacturing such as automotive, food and engineering, gave an example of Boeing Aerostructures Australia Limited monitoring the time it took workers to complete tasks and displaying these times against workers' names in the workplace for all to see (for more detail, go to Case Study 2.1).[11] It also raised the use of GPS tracking and cameras installed in work vehicles that employees are allowed to use outside of work for personal use, but which cannot be disconnected after hours.[12]

Other inquiries have reported that the real-time productivity of workers at Amazon is tracked through cameras, scanners and other devices such as smart wristbands used to move goods to set target pick rates and monitor workers' break times and

---

4 National Tertiary Education Union, *Submission 24*, p. 7.

5 Ibid., p. 8.

6 Ibid., p. 9.

7 United Workers Union, *Submission 25*, p. 10.

8 Finance Sector Union, *Submission 35*, p. 5.

9 Victorian Trades Hall Council, *Submission 28*, p. 13.

10 Ibid., p. 30; Building Industry Group of Unions, *Submission 36*, p. 1; Australian Nursing and Midwifery Federation, Victorian Branch, *Submission 38*, p. 4.

11 Australian Manufacturing Workers' Union, *Submission 31*, p. 13.

12 Ibid., pp. 13–14.

conversations with co-workers.[13] Media in late 2024 also reported how workers at Woolworths warehouses wear headsets that direct their tasks, set targets for how long the task should take and measure their productivity and length of bathroom breaks.[14] In both these situations, workers feel under pressure to meet set target rates and may avoid taking breaks to drink water or go to the toilet in case it affects their work rate, which could then influence the shifts they are offered going forward.[15]

Case Study 2.1 '[W]orkers were made to feel shamed and distressed'

'Using the aviation and defence company's case as an example … 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.

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.'

Source: Australian Manufacturing Workers' Union, *Submission 31*, p.17.

The Committee also heard that employees at the Commonwealth Bank of Australia (CBA) must download the *Navigate* app onto their personal devices to access buildings, book a workstation, register visitors and report faults; however, the app also continuously collects data on workers' precise location and some workers have been asked to apply for leave when they are away from their desk or appear unproductive.[16] In its submission, the CBA acknowledged that it uses mobile phone applications to monitor staff location as well as a range of other types of surveillance to monitor

---

13 Victorian Trades Hall Council, *VTHC submission to the Inquiry into the digital transformation of workplaces*, submission to House of Representatives Standing Committee on Employment, Education and Training, 2024, p. 18; Parliament of New South Wales, Legislative Council Select Committee on the Impact of Technological and Other Change on the Future of Work and Workers in New South Wales, *Impact of technological and other change on the future of work and workers in New South Wales: final report—workplace surveillance and automation*, November 2022, p. 15.

14 Ariel Bogle, "Stop all time wasting': Woolworths workers tracked and timed under new efficiency crackdown', *The Guardian*, 23 October 2024, <https://www.theguardian.com/business/2024/oct/23/woolworths-staff-efficiency-productivity-crackdown-timed> accessed 25 October 2024.

15 Victorian Government, *Submission 43*, p. 14.

16 Finance Sector Union, *Submission 35*, p. 7; Alysia Blackham, 'Surveillance, data collection and privacy at work: a new application of equitable obligations?', *Australian Journal of Labour Law*, (forthcoming), 2025, p. 2.

access to buildings, web browsing, emails and interactions with customers as well as to review the creation, access and deletion of all files on its information technology (IT) systems.[17]

Dr Jake Goldenfein, a Senior Lecturer at the University of Melbourne and Chief Investigator at the Australian Research Council Centre of Excellence for Automated Decision-Making and Society, added that any workplace that uses two-factor authentication can track its workers spatially through the worker's personal mobile phone while they are on premises.[18]

2.1.2 Technology and remote work have fuelled the rise in workplace surveillance

While workplace surveillance is not new, recent practices are significantly different, especially in terms of the intensity and extent of surveillance both at work and at home, and beyond work activities and working hours.[19] Surveillance and tracking devices have become cheaper, easier and more ubiquitous in the last decades.[20] In fact, surveillance has become so pervasive in modern society that it is now normalised with closed-circuit television (CCTV), live traffic cameras and geolocation tagging on mobile phones accepted as everyday features of modern life.[21] This section considers how technological capabilities and the changing nature of work have led to the growing intensity of workplace surveillance.

Workplace surveillance is easier as technology advances

Alongside the shift towards remote working and working from home that was accelerated during the lockdowns of the COVID-19 pandemic, there has been an increase in the supply and demand for workplace surveillance technologies, especially as they became cheaper and easier to install.[22] It is not only surveillance technologies that have become cheaper and easier, but also the collection of data and the software to interpret it and develop performance measures.[23] As the Finance Sector Union (FSU), which represents workers in banking, insurance, superannuation, financial planning

---

17 Commonwealth Bank of Australia, *Submission 44*, pp. 1–2.

18 Dr Jake Goldenfein, Senior Lecturer and Chief Investigator of ADM+S Centre (University of Melbourne node), ARC Centre of Excellence for Automated Decision-Making and Society, RMIT, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 51.

19 Dr Fiona Macdonald, Policy Director, Industrial and Social, Centre for Future Work, Australia Institute, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 18.

20 Office of the Victorian Information Commissioner, *Submission 39*, p. 2; Professor Peter Leonard, Principal, Data Synergies and Professor of Practice, UNSW Business School, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 5; Associate Professor Normann Witzleb, Faculty of Law, Monash University, and Faculty of Law, The Chinese University of Hong Kong, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 41.

21 Centre for Decent Work and Industry, QUT, *Submission 13*, p. 4; Eurofound, *Employee monitoring and surveillance: the challenges of digitalisation*, Publications Office of the European Union, Luxembourg, 2020, p. 47.

22 Finance Sector Union, *Submission 35*, p. 5; Office of the Victorian Information Commissioner, *Submission 39*, p. 2; Victorian Government, *Submission 43*, p. 13; Associate Professor Normann Witzleb, *Transcript of evidence*, p. 41.

23 Institute for Public Policy Research, *Watching me, watching you: worker surveillance in the UK after the pandemic*, report prepared by Henry Parkes, London, 2023, p. 7.

and finance, stated, 'there has been a steady increase in the types of surveillance being undertaken, the information being collected, and the conclusions drawn from it.'[24] This can have benefits in terms of training and workplace safety, but it can also have more detrimental effects, as explored further in Chapter 3.[25]

The Committee heard of a range of software programs that employers can purchase and deploy on their IT systems to collect large amounts of data, which can be fed into performance management and predictive analytic systems to monitor their employees.[26] Examples of these software programs, also known as bossware or tattleware, include:

- ActivTrack, DeskTime, eSurveiller, Flexispy, Hubstaff, Interguard, Kickidler, Spyera, Time Doctor, Teramind and Worksmart, which monitor keystrokes, login times, search histories and the time workers spend on various apps, and can take screenshots at set intervals and notify managers if data suggests an employee is distracted
- iMonitor, which in addition to the above capabilities can also take control of a computer remotely and turn on a computer's webcam to view the surroundings
- WorkExaminer, which can also record instant messaging activities and capture screenshots at regular intervals and then play them back like a movie
- Sneek, which constantly takes photos of workers through their laptop cameras every one to five minutes, with managers setting the frequency
- CallMiner, which records and transcribes telephone calls and uses AI to scan for certain words and phrases or to analyse how well a worker handled a call.[27]

Some of these software programs also 'integrate with payroll, project management and other systems.'[28] The United Workers Union, which represents workers across more than 45 industries, gave an example of a call centre worker who had 30 minutes of work deducted from his weekly earnings because he was away from his computer when a fire alarm in his apartment building went off and he was required to log off and evacuate.[29]

---

24 Finance Sector Union, *Submission 35*, p. 5.

25 Eurofound, *Employee monitoring and surveillance*, p. 7.

26 Dr Fiona Macdonald, *Transcript of evidence*, p. 18.

27 Centre for Decent Work and Industry, *Submission 13*, p. 5; Professor Peter Holland and Dr Jacqueline Meredith, Swinburne University of Technology, *Submission 22*, p. 7; Victorian Trades Hall Council, *Submission 28*, p. 14; Institute for Public Policy Research, *Watching me, watching you*, p. 9; Claire Brownell, 'The boss is watching', *Maclean's*, 15 December 2020, <https://macleans.ca/society/the-workplace-of-the-future-will-probably-remain-under-surveillance> accessed 12 June 2024; Benedict Collins, 'Best employee monitoring software of 2024', *TechRadar*, 4 July 2024, <https://www.techradar.com/best/best-employee-monitoring-software> accessed 17 July 2024; Danielle E. Thompson and Adam Molnar, 'Workplace surveillance in Canada: a survey on the adoption and use of employee monitoring applications', *Canadian Review of Sociology*, vol. 60, 2023, p. 813; Rogers, 'The law and political economy of workplace technological change', p. 568.

28 Kirstie Ball, *Electronic monitoring and surveillance in the workplace: literature review and policy recommendations*, Publications Office of the European Union, Luxembourg, 2021, p. 54.

29 United Workers Union, *Submission 25*, p. 13.

Other employers in the home-care sector use mobile phone apps such as CarelinkGO and Procura to give workers access to patient notes, tasks, maps and rosters but also record shift start and end times, determine how long a task should take and suggest the fastest travel routes between patients.[30] Technology firm Fujitsu has created an AI model that can detect small changes in a person's facial expressions to determine if they are concentrating, and wearable devices can now monitor wearer's conversations in terms of who they are speaking to, how enthusiastically they are speaking and how much time they spend talking and listening.[31]

Published research also identifies other developments in workplace surveillance including technologies that can monitor employees' thoughts, feelings and behaviours making more personal data visible to employers, and the move towards greater access into workers' personal lives, for example by employers providing workers with laptops and smartphones that can also be used outside of work for personal and social activities.[32]

Cameras are more ubiquitous in the workplace being routinely installed in delivery vehicles, taxis and corporate vehicles, as well as in classrooms, healthcare settings and home-based workplaces.[33] Other new technologies such as GPS and RFID tracking, micro-chip implants, automated video pattern recognition, biometric access control, AI, speech and body temperature tracking and emotion analytics are enabling more intrusive surveillance and the collection of data at a greater and more granular scale.[34]

Another new development that is expected to be readily adopted by workplaces within the next five years is neurosurveillance, which is the use of neurotechnology to determine employees' cognitive state such as their level of attention and effort. Neurotechnologies such as electroencephalograms (EEGs), which measure electrical activity in the brain, and transcranial direct current stimulation, which uses low-intensity electrical currents to modify brain activity, are currently used in Australian workplaces such as mines to monitor attention and fatigue. Other neurotechnologies exist that can decode mental images and intended speech, and these could also be introduced to workplaces in the future to understand employees' minds and modify their work performance.[35]

---

30 Ibid., pp. 14–15.

31 Institute for Public Policy Research, *Watching me, watching you*, p. 11; Murray Brown and Normann Witzleb, 'Big brother at work: workplace surveillance and employee privacy in Australia', *Australian Journal of Labour Law*, vol. 34, no. 3, 2021, pp. 21–22.

32 Ball, *Electronic monitoring and surveillance in the workplace*, p. 6; Peter Leonard, 'Workplace surveillance and privacy', *Computers and Law: Journal for the Australian and New Zealand Societies for Computers and the Law*, vol. 93, 2021, p. 65; Thompson and Molnar, 'Workplace surveillance in Canada', p. 803.

33 Ball, *Electronic monitoring and surveillance in the workplace*, p. 26.

34 Joanna Bronowicka, et al., *'Game that you can't win'?: workplace surveillance in Germany and Poland*, European University Viadrina, Frankfurt, 2020, p. 31; Eurofound, *Employee monitoring and surveillance*, p. 5; Thompson and Molnar, 'Workplace surveillance in Canada', p. 803.

35 Australian Human Rights Commission, *Protecting cognition: background paper on human rights and neurotechnology*, Sydney, 2024, p. 35; Dr Allan McCay, Academic Fellow, Sydney Law School, University of Sydney, Co-Director, The Sydney Institute of Criminology and President, Institute of Neurotechnology and Law, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 7.

Neurosurveillance can be beneficial for safety reasons, especially for jobs that require high or sustained levels of concentration, but using it to boost productivity, for billing purposes (to measure billable units of attention) and for hiring, promoting and firing staff has the potential to be problematic and in some cases discriminatory if it overlooks other relevant factors such as empathy and creativity.[36] The use of neurosurveillance at work is gaining attention around the world, with the Organisation for Economic Co-operation and Development and the Australian Human Rights Commission developing policies and publishing papers on its impact on human rights, especially the rights to mental privacy and integrity.[37]

Employers want more surveillance as remote working grows

The Committee heard about 'productivity paranoia' where employers are sceptical that their workers are productive when out of their sight; in fact, 85% of leaders in Microsoft's 2022 Work Trend Index survey said they had trouble believing workers were productive when working remotely.[38] 'Productivity paranoia' has led to the 'flexibility paradox', where supervisory control increases with higher levels of flexibility such as hybrid and remote working.[39] This usually manifests as electronic monitoring and surveillance of employees, who feel their managers 'hold themselves to different … standards' and are not 'monitored in the same way'.[40]

Demand for workplace surveillance software surged in 2020 as the COVID-19 pandemic forced people worldwide to shift to remote work. From April 2019 to April 2020, global demand for workplace surveillance software grew by 108% and search engine queries for 'how to monitor employees working from home' increased by 1,705% over the same period. Software providers also reported concurrent increases in sales inquiries; for example, DeskTime reported a 333% increase, Time Doctor 202%, Teramind 169% and Kickidler 139%.[41]

Similar growth was seen in Australia, with media reports stating that sales of surveillance software soared 300% in the two months prior to May 2020.[42] Technology research consultancy Gartner found that by the end of 2020, up to 80% of organisations worldwide and 90% in Australia were using some form of electronic surveillance to monitor remote workers.[43] Growth in workplace surveillance search engine queries was sustained beyond the pandemic; in September 2022, searches for

---

36 Dr Allan McCay, *Transcript of evidence*, p. 8; Australian Human Rights Commission, *Protecting cognition*, p. 35.

37 Eurofound, *Employee monitoring and surveillance*, p. 8; Australian Human Rights Commission, *Protecting cognition*, p. 3.

38 Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 6; Kate Morgan and Delaney Nolan, 'How worker surveillance is backfiring on employers', *BBC*, 30 January 2023, <https://www.bbc.com/worklife/article/20230127-how-worker-surveillance-is-backfiring-on-employers> accessed 15 May 2024.

39 Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 6.

40 Victorian Trades Hall Council, *Submission 28*, p. 21.

41 Ball, *Electronic monitoring and surveillance in the workplace*, p. 12; Thompson and Molnar, 'Workplace surveillance in Canada', p. 804.

42 Victorian Government, *Submission 43*, p. 14.

43 Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 5.

'how to monitor employees working from home' was 383% higher than the pre-pandemic baseline and searches for 'best employee monitoring software' was 201% higher than the baseline.[44]

Employers had genuine security reasons for implementing surveillance software during the pandemic so they could ensure that the person accessing company systems remotely was a genuine worker authorised to access the system and not a hacker or someone impersonating an employee. However, as lawyer and data and technology business consultant Professor Peter Leonard told the Committee:

> it is probably fair to say that many employers did not properly understand the types of controls and safeguards they should be implementing as to how and when those technologies were used, limiting access to relevant surveillance information within the organisation, and were not taking proactive steps to inform employees that they were being surveilled in this way.[45]

This rapid adoption of workplace surveillance software was suboptimal because employers had limited time to consider the relevant legal and privacy implications and to consult with their employees. At the same time, workers were worried about their job security and were not informed enough about the implications of such surveillance, so they were not well placed to resist.[46]

Thus, the pandemic became a catalyst for using technology to shift the nature of work from 'workplace' to 'workspace', blurring the boundaries between work and home life and eroding the privacy of workers' homes and families.[47] Prior to the pandemic, remote working was a rare benefit often preserved for senior workers in high-skilled professions but suddenly many workers were given access to it.[48]

As surveillance measures increased in response to the growth of remote working, managers and supervisors may not have been adequately skilled to monitor people working remotely, and workers reported that the technology placed pressure on them to be seen as 'always on', that is, constantly working.[49] Some observers have suggested that the pandemic has created a situation where technological surveillance is normalised in the workplace despite the threats to workers' rights and privacy.[50]

FINDING 1: While workplace surveillance has a long history, advances in surveillance technology and the pandemic-induced shift to remote working has made workplace surveillance easier, cheaper and more pervasive in Victorian workplaces.

---

44 Institute for Public Policy Research, *Watching me, watching you*, p. 10.

45 Professor Peter Leonard, *Transcript of evidence*, p. 5.

46 Institute for Public Policy Research, *Watching me, watching you*, p. 11.

47 Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 2.

48 Ibid., p. 3; Ball, *Electronic monitoring and surveillance in the workplace*, p. 51.

49 Ball, *Electronic monitoring and surveillance in the workplace*, pp. 52, 54.

50 Institute for Public Policy Research, *Watching me, watching you*, p. 5; Brownell, 'The boss is watching'; Ahmed Maati, 'Long-term prescription?: digital surveillance is here to stay', *Czech Journal of International Relations*, vol. 56, no. 4, 2021, p. 113.

2.2 Artificial intelligence is increasingly used in workplace surveillance

The Committee heard that the latest significant development in workplace surveillance is the use of AI to process the data and make automated decisions about workers and the workplace using algorithms, also known as algorithmic decision-making. This advanced form of surveillance has created a level of worker monitoring and data gathering and processing that is much greater than ever envisaged before.[51] AI, specifically generative AI, is technology that can perform tasks such as generating content, forecasts and decisions independently of humans. AI systems require data sets to train the model that generates these outputs.[52]

According to a survey of 487 of its members, the Victorian Branch of the Community and Public Sector Union (CPSU), which represents workers in the Victorian public service and public authorities and agencies, found 37% of respondents stated AI was currently being used in their workplaces and 38% said they were not sure. When asked if their workplace had a policy on the use of AI at work, 11% said yes, 24% said no and 57% were unsure.[53]

In the workplace, AI can be beneficial for detecting, reporting and rectifying safety incidents or hazards that might go underreported by humans, such as early signs of equipment failures.[54] Other tasks that employers may use AI for include predicting staffing and resourcing needs, optimising or automating labour-intensive processes, coordinating the sequence of production tasks, anticipating maintenance and replacement needs, and matching labour inputs and outputs with fluctuating consumer demand.[55] In the best case scenario, AI systems help employers save time and money and reduce the risks of human bias and human error by making objective automated decisions.[56]

In terms of staff management, AI surveillance systems gather data about employees and their work, then sort, analyse and process this data to inform or determine decisions across the employment life cycle, from recruitment to work allocation, work assessment, and termination.[57] Employers can use AI surveillance systems to evaluate employee performance, monitor content of emails and other digital communications,

---

51 The Centre for Future Work, Australia Institute, *Submission 32*, p. 2; Finance Sector Union, *Submission 35*, p. 8; Professor Peter Leonard, *Transcript of evidence*, p. 5; Associate Professor Penelope Williams, Director, Centre for Decent Work and Industry, QUT, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 22; Thomas Kalischko and René Riedl, 'Electronic performance monitoring in the digital workplace: conceptualization, review of effects and moderators, and future research opportunities', *Frontiers in Psychology*, vol. 12, 2021, p. 2, doi: 10.3389/fpsyg.2021.633031; Victorian Trades Hall Council, *VTHC submission to the Inquiry into the digital transformation of workplaces*, p. 3.

52 Cole Stryker and Eda Kavlakoglu, 'What is artificial intelligence (AI)?', *IBM*, 9 August 2024, <https://www.ibm.com/think/topics/artificial-intelligence> accessed 13 December 2024; Peter McDonald, 'Robodebt is just one reason why we should be worried about AI', *Centre for Social Impact*, 14 August 2023, <https://www.csi.edu.au/news/robodebt-is-just-one-reason-why-we-should-be-worried-about-ai> accessed 13 December 2024.

53 Community and Public Sector Union, Victorian Branch, *Submission 20*, p. 6.

54 Australian Industry Group, *Submission 40*, p. 7.

55 Victorian Trades Hall Council, *VTHC submission to the Inquiry into the digital transformation of workplaces*, p. 4.

56 Alysia Blackham, 'Setting the framework for accountability for algorithmic discrimination at work', *Melbourne University Law Review*, vol. 47, no. 63, 2023, p. 68.

57 Ibid., pp. 67–68.

and assess the quality and sentiment of workers' interactions with clients or colleagues by measuring tone of voice, language used and facial expressions.[58] See Case Study 2.2 as an example.

Case Study 2.2 'That triggered the AI to say there is actually a problem'

'[O]ne of our members was having a conversation—they are a financial adviser for one of the big employers in our sector—with a member of their organisation. Building rapport at the start of the conversation they said, 'Unfortunately it's been really rainy lately,' and the overall sentiment of that conversation was marked as a sad face, and that was because when we went back and drilled down into what the issue was with the conversation—otherwise it was a very positive, productive conversation—it was because they had used the word 'unfortunately'. That triggered the AI to say there is actually a problem here and the sentiment of the conversation is a negative one. Of course, when we sat down as part of a disciplinary process and listened to that recording, it was very clear that there was no sentiment problem with that conversation at all. But the enormous issue with that, or one of the enormous issues with that, is that it means that there is a disciplinary process that one of our members is subject to, and we all know the enormous stress of being involved in a disciplinary process; even if it ultimately turns into nothing, it is still a really difficult thing to go through. And we also know that a lot of workers who might not have the benefit of being a union member unfortunately go into that situation on their own; they do not know that they can ask for the recording, and they often just cop the consequence even if it is entirely unfair.'

Source: Nicole McPherson, National Assistant Secretary, Finance Sector Union, public hearing, Melbourne, 3 September 2024, *Transcript of evidence,* p. 41.

Employers can also use workers' surveillance data to train algorithmic decision-making software, to better understand and influence workers, and to identify production points that could be optimised.[59] According to the NTEU, this data is also being used in knowledge industries to 'expropriate value from workers' such as their intellectual property.[60] One of its members said that academics are told their lectures will be recorded and stored, with the content becoming the university's intellectual property and available for use by AI in the future.[61]

AI analysis of workplace surveillance data combined with findings from psychological studies can also provide employers with intimate knowledge about their workers and even predict their future behaviours, for example, their sleep and fitness habits, personality traits, work satisfaction, and the likelihood of them being disobedient,

---

58 Victorian Trades Hall Council, *Submission 28*, p. 10; Office of the Victorian Information Commissioner, *Submission 39*, p. 8; Dr Fiona Macdonald, *Transcript of evidence*, p. 20.

59 Victorian Trades Hall Council, *VTHC submission to the Inquiry into the digital transformation of workplaces*, p. 11.

60 National Tertiary Education Union, *Submission 24*, p. 5.

61 Ibid., p. 10.

getting sick, falling pregnant, staying at the organisation long term or becoming a leader.[62] Any information suggesting a risk to the organisation can be used to rank employees.[63] According to Fiona Macdonald, who is a Policy Director with the Centre for Future Work at the Australia Institute:

> Workers' futures will be determined on the basis of those kinds of analyses. Nobody has any idea how fair that is, and there is good evidence that it is not.[64]

User and entity behaviour analytics, or UEBA, software can create detailed profiles of workers' behaviour such as their login patterns, how they use different applications, the information they access, their sick leave and social interactions. This behavioural profile can be assessed against a baseline profile to determine any future threats to the organisation, even if these assumptions and conclusions may be incorrect or circumstantial.[65] As Dr Jean Linis-Dinco, who completed her PhD on the use of machine learning techniques, told the Committee:

> these AI-driven systems we know that they are not infallible. They rely on patterns and data which can lead to incorrect assumptions. An algorithm might flag a well-intentioned action as, let us say, suspicious simply because it deviates from the majority or deviates from what is expected or what is normal and not because it poses any real threat. And the consequences of such false positives are not trivial. They can affect a worker's performance reviews, professional relationships and even their career trajectory.[66]

The Centre for Future Work has argued that technology using algorithmic decision-making is not a neutral process, and while it could be used to optimise work practices to help workers focus on more creative tasks, it can also be used to displace workers. It quoted results from a 2023 global survey of IT professionals for the IBM Global AI Adoption Index that showed the most common reason organisations use AI is to automate customer services (47%), with only 34% of organisations training or reskilling their employees to work with AI tools.[67]

Not only might AI automate jobs, but it can also undermine the quality of existing jobs through constant surveillance and dehumanise workers by forcing them to interact with automated processes.[68] This can occur when management functions such as rostering and task allocation are outsourced to digital devices using algorithmic decision-making.[69] Further concerns about the use of AI with workplace surveillance are discussed below.

---

62 Victorian Trades Hall Council, *VTHC submission to the Inquiry into the digital transformation of workplaces*, p. 12; Brown and Witzleb, 'Big brother at work', p. 22.

63 Associate Professor Penelope Williams, *Transcript of evidence*, p. 22.

64 Dr Fiona Macdonald, *Transcript of evidence*, p. 20.

65 Dr Jean Linis-Dinco, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 23; Community and Public Sector Union, *Submission 20*, p. 5.

66 Dr Jean Linis-Dinco, *Transcript of evidence*, p. 23.

67 Dr Fiona Macdonald and Dr Lisa Heap, Centre for Future Work, Australia Institute, *Inquiry into the digital transformation of workplaces*, submission to House of Representatives Standing Committee on Employment, Education and Training, 2024, p. 2.

68 Blackham, 'Setting the framework for accountability for algorithmic discrimination at work', p. 69.

69 Lauren Kelly, Research and Policy Officer, United Workers Union, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 47.

2.2.1 Using AI with workplace surveillance has risks of bias and unfairness

A research paper that explores the regulatory mechanisms around the use of AI with workplace surveillance stated:

> A great many claims have been made about the potential benefits AI might offer. Many of these feature vague explanations of the process whereby the benefits would arise. A proportion of the claims have some empirical evidence to support them, but many are mere assertions in media releases, without the support of independent testing.[70]

While it was not an AI system, the author used the example of the Australian Government Robodebt scandal, where an automated system issued erroneous debt notices to welfare recipients based on incorrect calculations and assumptions.[71] Others have noted the risk posed by AI is that it 'adds a layer of sophistication to automated decision-making', such as the type that was used for Robodebt.[72] The risks of AI systems can be minimised if they are used appropriately and have effective inbuilt safeguards against misinterpretation. For example, if low-quality facial recognition technology refuses access to a legitimate worker, then an alternative mechanism such as a password could be used. But without such safeguards, there is a high risk for errors and serious harm.[73]

The Office of the Victorian Information Commissioner, which regulates the collection, use and disclosure of personal information in the Victorian public sector, stated that the potential risks of using AI systems include discrimination, bias and inequality if the model or algorithm has inbuilt bias that exacerbates existing social prejudices.[74] AI systems can also generate 'AI hallucinations' where the information they produce is incorrect or misleading. This may be due to the input of poor training data into the model or the model making incorrect assumptions. AI bias and hallucinations can be difficult to recognise, potentially resulting in unfair treatment of employees.[75]

According to the Australian Government Department of Industry, Science and Resources, which published its Voluntary AI Safety Standard in 2024, traditional software systems are easy to control, predict and understand whereas AI systems, which often outperform traditional systems, are riskier because the models behind them are less transparent, harder to interpret and more complicated to verify.[76]

---

70 Roger Clarke, 'Responsible application of artificial intelligence to surveillance: what prospects?', *Information Polity*, vol. 27, no. 2, 2022, p. 180.

71 Ibid., p. 187.

72 McDonald, 'Robodebt is just one reason why we should be worried about AI'.

73 Clarke, 'Responsible application of artificial intelligence to surveillance', pp. 180–181.

74 Office of the Victorian Information Commissioner, *Submission 39*, p. 8; Institute for Public Policy Research, *Watching me, watching you*, p. 21.

75 Office of the Victorian Information Commissioner, *Submission 39*, p. 8.

76 Department of Industry, Science and Resources, National Artificial Intelligence Centre, *Voluntary AI safety standard*, Australian Government, August 2024, p. 6.

The speed with which AI can process workplace surveillance data can result in incorrect or misrepresentative conclusions, which is problematic because this space is currently unregulated.[77] See Chapter 4 for further discussion on the regulation of the use of AI with surveillance data.

Most of the problems with AI are due to algorithmic bias, where an AI system makes errors and produces unfair or discriminatory results, which can be unjust if these results are used for recruitment or promotions. This might be due to the design of the model, but more likely the data used to train it, which itself may be biased, discriminating according to characteristics such as gender, ethnicity, age, ability or sexual orientation.[78] Algorithmic bias is hard to identify because the algorithms are complex and the basis for their decisions are unknown and often unexplainable.[79] Without ethical principles or transparency the dangers of AI are significant.[80]

For example, AI systems used for recruitment purposes will be trained with an employer's previous hiring data. The system may pick up patterns in the employer's recruitment, such as a preference for applicants with higher levels of education or who are early in their career, which could result in recruitment decisions that give too much emphasis on irrelevant factors or that discriminate against certain groups.[81]

Adjunct Professor Moira Paterson from the Castan Centre for Human Rights Law, an academic centre at Monash University that conducts research into human rights, explained to the Committee how bias in AI systems can result in unfair outcomes:

> Essentially you have to feed the machine lots of examples so that it learns. Sometimes data about specific groups is lacking, just historically or whatever, and so that means it may be less accurate in respect to them. It may mean that it discriminates, not from any deliberate programming but just because that has happened. What is happening there, as I say, is happening in a so-called black box, because even the people who design that decision-making software themselves would have difficulty explaining how it arrives at a particular decision, because a lot of the modern automated decision-making relies on the machine itself learning and changing as more and more data is fed into it, so it is not just putting in a simple equation and then getting it to act on that. There might be that at the beginning, but then the machine goes off in directions using neural networks and so forth, and that means that you have got very important decisions affecting individuals being made in a way that is difficult to explain. I can well understand that

---

77 Nicole McPherson, National Assistant Secretary, Finance Sector Union, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 41.

78 Community and Public Sector Union, *Submission 20*, p. 9; Adjunct Professor Moira Paterson, Castan Centre for Human Rights Law, Faculty of Law, Monash University, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 46; Ball, *Electronic monitoring and surveillance in the workplace*, p. 73; Institute for Public Policy Research, *Watching me, watching you*, p. 18; Australian Human Rights Commission, *Using artificial intelligence to make decisions: addressing the problem of algorithmic bias*, report prepared by Finn Lattimore, Simon O'Callaghan, Zoe Paleologos, Alistair Reid, Edward Santow, Holli Sargeant and Andrew Thomsen, Sydney, 2020, p. 5.

79 Institute for Public Policy Research, *Watching me, watching you*, p. 5; Macdonald and Heap, *Inquiry into the digital transformation of workplaces*, p. 6.

80 Wendi S. Lazar and Cody Yorke, 'Watched while working: use of monitoring and AI in the workplace increases', *Reuters*, 26 April 2023, <https://www.reuters.com/legal/legalindustry/watched-while-working-use-monitoring-ai-workplace-increases-2023-04-25> accessed 16 May 2024.

81 Ibid.

> if you are an employee whether or not you get promoted, or for a potential employee whether you get employed, and all sorts of other things—assessments about your performance—if these things are all automated, there can be a lot of unfairness there.[82]

Since the data scientists and engineers leading the development of AI are largely young, white men, gender and cultural disparities are prone to be built into the systems from the training data, either purposely or inadvertently.[83] These data scientists and engineers building the systems are unlikely to take any responsibility for the decisions made by the algorithms and instead will shift the responsibility to the employer that uses the system. This creates an accountability vacuum, where there is no way to critically review the AI process, and employers can point to the algorithm if accused of discrimination.[84]

Unions such as the CPSU and FSU find the lack of accountability and transparency around the use of AI with workplace surveillance concerning.[85] The FSU was particularly concerned about the use of AI systems to analyse recordings of their members interacting with customers or colleagues to draw potentially erroneous conclusions about the sentiment of the interaction or the quality of their work.[86] It notes that employees are rarely informed that AI is analysing their written or verbal communications and making inferences from the data.[87] Even if employees question these decisions, employers are unable to explain the AI system's decision-making process, or in some cases they 'refuse to disclose [the information], citing that it is "proprietary" or "confidential".'[88] While the FSU sees the value of AI systems identifying cases of inappropriate behaviour or policy breaches, it stressed the importance of having a human review the evidence first, prior to the employer taking any disciplinary action.[89]

FINDING 2: Employers are increasingly using artificial intelligence to process surveillance data and make conclusions about workers' behaviour, sentiment and performance, which could result in unfair outcomes if the decisions are based on inaccurate assumptions or interpretations.

2.3 Victorian employees are rarely informed about surveillance practices

A common theme in the evidence was Victorian employers' lack of transparency around the workplace surveillance they use and how they use it, especially when there

82 Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 46.

83 Blackham, 'Setting the framework for accountability for algorithmic discrimination at work', p. 72.

84 Ibid., p. 78; Institute for Public Policy Research, *Watching me, watching you*, p. 18.

85 Community and Public Sector Union, *Submission 20*, p. 3; Finance Sector Union, *Submission 35*, p. 8.

86 Finance Sector Union, *Submission 35*, pp. 6–7.

87 Ibid., p. 8.

88 Ibid., pp. 4, 8.

89 Ibid., p. 11.

is no legal requirement to inform their staff.[90] For example, 81% of respondents to the VTHC survey stated that their employer had not discussed surveillance methods with them before they were implemented, and only 1% were given the chance to opt out of surveillance, suggesting that meaningful consultation and genuine consent were rare.[91] The NTEU survey found similar results with 82% of respondents reporting their employer did not notify them of workplace surveillance practices and 91% stating they were not consulted about these practices.[92]

This section considers the extent to which Victorian employers are informing their workers of the types of surveillance they use and how they use it. It concludes by exploring how surveillance that is implemented for one purpose then gets used covertly for other purposes, also known as function creep.

2.3.1 Victorian employees are unaware of the full extent of workplace surveillance

As Chris Molnar, who co-chairs the Workplace Relations Committee at the Law Institute of Victoria, the state's peak body for lawyers, stated:

> You do not know what is happening in Victoria. There is simply an obligation on the employer not to do certain surveillance in certain situations, but employees in Victoria are not aware of what surveillance is taking place. We see that as a gap.[93]

Amy Salmon, Principal Psychological Health and Safety Specialist at WorkSafe Victoria, the state's workplace health and safety authority, added that when employees contact them about workplace surveillance, it is often because they have been given little information about the surveillance from their employers and there are no relevant policies and procedures in place.[94]

There was also a significant proportion of workers who were unsure if their employers were conducting surveillance in the workplace, which also suggests a lack of transparency. For example, 21% of VTHC survey respondents were unsure, as were 35% of NTEU survey respondents and 40% of respondents to a member survey run by the Victorian and Tasmanian Authorities and Services Branch of the Australian Services Union (ASU), which represents workers in local government, social and community services, energy, water, transport and public authorities.[95]

---

90 See for example, Centre for Decent Work and Industry, *Submission 13*, p. 6; Construction, Forestry and Maritime Employees Union, Manufacturing Division, *Submission 17*, p. 2; United Workers Union, *Submission 25*, p. 17; Victorian Trades Hall Council, *Submission 28, Appendix*, p. 3; Finance Sector Union, *Submission 35*, p. 4; Australian Nursing and Midwifery Federation, *Submission 38*, pp. 2–3; Australian Services Union, Victorian Private Sector Branch, *Submission 41*, p. 4.

91 Victorian Trades Hall Council, *Submission 28*, p. 33; Oscar Kaspi-Cruchett, Researcher, Victorian Trades Hall Council, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 35.

92 National Tertiary Education Union, *Submission 24*, p. 11.

93 Chris Molnar, Co-Chair, LIV Workplace Relations Committee, Law Institute of Victoria, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 27.

94 Amy Salmon, Principal Psychological Health and Safety Specialist, WorkSafe Victoria, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 23.

95 National Tertiary Education Union, *Submission 24*, p. 7; Victorian Trades Hall Council, *Submission 28*, p. 14; Australian Services Union, Victorian and Tasmanian Authorities and Services Branch, *Submission 29*, p. 4.

The NTEU also found that 48% of respondents to its survey did not know if they were being surveilled while working from home and 60% did not know whether the data collected through surveillance was being used for specific purposes. In addition, most workers were not aware of their employer having a published policy on workplace surveillance, with 52% reporting no such policy existed and 43% unsure if one existed.[96] Similarly, the Australian HR Institute, the professional body that supports human resources in Australia, polled its members and found only 41% of the 59 respondents said their organisation had a workplace surveillance policy and requested employees' consent for surveillance, suggesting a lack of transparency in most workplaces.[97]

The CBA told the Committee it notifies its staff of the workplace surveillance it conducts through their contract of employment, which refers to relevant policies such as its Code of Conduct and Group Conduct Policy that outline the policy requirements for monitoring and workplace surveillance. The Enterprise Agreement also requires the CBA to consult with its staff about any major changes to surveillance that are likely to have a significant impact on employees.[98]

However, the Committee also heard from Tash Wark, Secretary of the Victorian and Tasmanian Authorities and Services Branch of the ASU, that notification of workplace surveillance:

> cannot just be a hidden line in a contract or a policy that you sign on that first day when you are kind of thrust with probably a whole lot of links to a data piece somewhere.[99]

The Australian Lawyers Alliance, a national association of lawyers, academics and other professionals dedicated to protecting the rights of the individual, agreed, adding that even though the employment contract might state that surveillance will occur and how, it rarely stated how the collected data will be used and stored. It also said that it was rare for Victorian employers to voluntarily disclose their workplace surveillance practices to their employees.[100]

Even when employers disclose that workplace surveillance is occurring, they might not provide other relevant information such as the specific forms of surveillance used, how the data might be used for performance management, and what recourse workers have if they feel the surveillance is too intrusive, negatively affecting their health or not being used for the intended purposes.[101]

Some unions mentioned how their members often only discover workplace surveillance is occurring when the data is used as part of a disciplinary or performance management process for themselves or their co-workers.[102] Nicole McPherson, National

---

96 National Tertiary Education Union, *Submission 24*, p. 11.

97 Australian HR Institute, *Submission 10*, p. 4.

98 Commonwealth Bank of Australia, *Submission 44*, pp. 2, 3.

99 Tash Wark, Secretary, Australian Services Union, Victorian and Tasmanian Authorities and Services Branch, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 44.

100 Australian Lawyers Alliance, *Submission 7*, p. 6.

101 Centre for Decent Work and Industry, *Submission 13*, p. 7; Victorian Trades Hall Council, *Submission 28*, p. 12.

102 Finance Sector Union, *Submission 35*, p. 9; Australian Services Union, Victorian Private Sector Branch, *Submission 41*, p. 4.

Assistant Secretary of the FSU, said that in addition to finding out about workplace surveillance when it arises as part of a disciplinary process, it might also be revealed unexpectedly through public statements by business groups, such as the Business Council of Australia, that might talk about how its members are using surveillance, or AI based on surveillance data, in a certain way.[103]

Some employers might seek their employees' consent to workplace surveillance, but if the only way to perform the work is to use the employers' devices, software and systems, consent may not be voluntary especially if refusal means the loss of employment. Furthermore, if employers do not provide substantive details about how the surveillance will be conducted and how the data will be handled, genuine consent cannot be given and there is no way for employees to check if the surveillance is being used as stated.[104] Chapter 3 covers the issue of consent in more detail.

The vast majority (92%) of respondents to the ASU's survey agreed that employers should tell their employees when they use any form of electronic or digital surveillance.[105] Research also shows that being transparent about workplace surveillance increases employees' perceptions of fairness, justice and job satisfaction and results in greater trust in management and reduced turnover.[106]

FINDING 3: Employers in Victoria are seldom fully transparent about their surveillance practices so many workers are unaware of the extent of surveillance in their workplace and how their employers are using the associated data.

2.3.2 Undisclosed function creep is problematic

Workplace surveillance for safety or training purposes is more acceptable to employees than surveillance for performance management or for no clear purpose. Employees also feel uncomfortable when employers begin to use information from surveillance for a purpose different to which it was initially obtained without their knowledge, also known as function creep.[107] For example, this can occur when the data obtained from surveillance technology installed for security purposes begins to be used to analyse workers' performance under the rationale of productivity or efficiency.[108] See Case Study 2.3 for another example.

---

103 Nicole McPherson, *Transcript of evidence*, p. 40.

104 Centre for Decent Work and Industry, *Submission 13*, p. 7; Rachel Dixon, Privacy and Data Protection Deputy Commissioner, Office of the Victorian Information Commissioner, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 12.

105 Australian Services Union, Victorian and Tasmanian Authorities and Services Branch, *Submission 29*, p. 4.

106 Ball, *Electronic monitoring and surveillance in the workplace*, p. 17.

107 Ibid., p. 7; Bronowicka, et al., *'Game that you can't win'?*, p. 9.

108 Institute for Public Policy Research, *Watching me, watching you*, p. 9; Morgan and Nolan, 'How worker surveillance is backfiring on employers'; Kenneth McLeod, *Submission 2*, p. 1.

Case Study 2.3 'My state manager would routinely track field staff'

'I work for a Multi-National Company that in the last few years has installed Vehicle Tracking devices in the fleet cars of its field staff in Australia. The main reason given to us for this monitoring was for our safety if we got into an accident or we went missing etc. so our managers would be able to locate us. I actually was involved in a car crash last year in a work car but this tracking was never used in conjunction with the crash. My state manager would routinely track field staff just … because he could. He would use it for work place compliance and would use it as a tool to use against anyone he felt was not doing what we wanted them to be doing. In short, we felt that our privacy was being breached and the information gathered was being misused, resulting in a complete lack of trust and respect between us and our manager. I felt so strongly about this abuse of power that I actually resigned from my job of many years because of it.'

Source: Name withheld, *Submission 4*, p. 1.

Function creep is aided by advances in digital surveillance technology that is versatile and lends itself to a range of purposes, so a surveillance measure that was introduced for a fairly benign reason then has the potential to be used covertly for other reasons, which is seen as problematic.[109] Coupled with no legal obligation to limit the use of surveillance technology to a stated purpose or to inform workers of such changes, employers can use surveillance data gathered for one reason for other purposes with impunity, sometimes resulting in disciplinary outcomes for workers or dismissal.[110]

Stakeholders provided the Committee with specific examples. Fiona Macdonald from the Centre for Future Work spoke of her work with home-care workers who must use a mobile phone app for work appointments, but this app can also track their location and conversations, as can cameras in their vehicles, which were initially installed for safety purposes.[111] The Victorian Branch of the Australian Nursing and Midwifery Federation, which represents nurses, midwives and personal care workers, added that employers are using work apps to track and time nurses and midwives providing in-home care and questioning them about their travel activities, the time they took caring for patients and the time that passed between patients. This has resulted in workers forgoing breaks, doing administrative work in their vehicles, experiencing psychological stress and being subjected to disciplinary processes based on misinterpreted data.[112]

---

109 Eurofound, *Employee monitoring and surveillance*, p. 43.

110 Centre for Decent Work and Industry, *Submission 13*, p. 6; Susan Accary, President, Victoria Branch Committee, Australian Lawyers Alliance, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 27; Dr Dale Tweedie, Senior Lecturer, Department of Accounting and Corporate Governance, Macquarie University, public hearing, 26 September 2024, *Transcript of evidence*, p. 15.

111 Dr Fiona Macdonald, *Transcript of evidence*, p. 19.

112 Australian Nursing and Midwifery Federation, Victorian Branch, *Hearing notes*, supplementary evidence received 1 November 2024, p. 1.

The Postal and Telecommunication Branch Victoria of the Communications Workers Union (CWU), which represents workers in the telecommunications and postal industries, also spoke of Australia Post's introduction of CCTV, telematics and AI surveillance for security and safety purposes, but employees are reporting that Australia Post now uses these technologies to monitor their behaviour, whereabouts and performance, sometimes leading to discipline and even dismissal. This has made its 'members anxious, nervous, and intimidated and at times causing emotional distress.'[113] As Troy McGuinness, an Elected Organiser with the CWU, explained:

> We generally get told that these things are going to be put in (1) for the workers' safety and (2) for security. That is when they first implement it, and now we are five or six years down the road, more and more it gets used for discipline purposes. I have had many conversations with senior managers saying, 'Well, how is it that this has come about? Why are we even looking at it? You were meant to be investigating this.' They go, 'Well, when we were investigating it and we looked through it, we saw stuff that we couldn't unsee, so now we have to address that.' When you read the wording of your policy, you are meant to use this as a tool to be able to educate workers, let them know that they have done something unsafe and this is where they need to try and address safety and give them the opportunity to rectify the situation or change their behaviours. But no, what we find more and more nowadays is they look at the telematics for reasons they are not meant to be looking at them for, and then they are putting our members straight on a disciplinary inquiry and then using HR to back them up, to try and dismiss people for basically just going about the same job that they have done for the last 25 or 30 years.[114]

Other examples the Committee heard were:

- the use of cloud-based software such as Microsoft 365, which provides advanced security for organisations' IT systems, but also collects data that determines the time workers spend on emails and on different apps[115]
- geo-location tracking devices worn by miners and transport workers for safety purposes used to monitor when workers take breaks and if they deviate from their usual route[116]
- audio devices worn by casino security officers for safety and liability issues now used to monitor workers' conversations with each other and discipline them for unacceptable comments[117]

---

113 Communications Workers Union, Postal and Telecommunication Branch Victoria, *Submission 19*, p. 1; Leroy Lazaro, Branch Secretary, Communication Workers Union, Postal and Telecommunication Branch Victoria, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 44.

114 Troy McGuinness, Elected Organiser, Communication Workers Union, Postal and Telecommunication Branch Victoria, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 45.

115 Centre for Decent Work and Industry, *Submission 13*, p. 5.

116 Ibid., p. 6.

117 United Workers Union, *Submission 25*, p. 11.

- an informal chat between co-workers held on Microsoft Teams about an impending organisational restructure used to accuse a worker of undermining the employer and of not behaving in line with the organisations' values.[118]

The Victorian Information Commissioner, Sean Morrison, identified function creep as one of the risks of workplace surveillance that 'is a significant concern because it is gradual and hard to detect but has serious consequences for employees, in some cases putting their health and safety at risk.'[119] Further risks occur when employers over-collect data, have vague data retention policies, or the person responsible for data privacy leaves an organisation and there are no proper procedures for data handling.[120]

Several unions gave examples of workers being disciplined or terminated based on surveillance data collected for alternative purposes.[121] The Committee heard of cases where employers retroactively reviewed surveillance footage or keystrokes of a particular worker until they found an infraction such as a safety violation or taking an extended break that was subsequently used to discipline or terminate an employee. Overcollection of data, function creep and the lack of transparency call into question the procedural fairness of such disciplinary processes.[122]

The Victorian Private Sector Branch of the ASU, which represents workers in the private sector across a range of industries, also mentioned that employers are using surveillance data to threaten worker misconduct when the issue would be better described as underperformance and could be managed through performance discussions rather than disciplinary threats.[123] Dr Dale Tweedie, Senior Lecturer at Macquarie University whose research looks at the impact of workplace surveillance on workers, said the use of surveillance data for decision-making purposes is problematic because it relies on metrics that can miss nuances and may be invalid or unreliable when considered in isolation.[124]

Some academics have suggested that the use of surveillance as a tool for discipline or termination has shifted the employee management approach from positive incentives to negative punishments. The pervasiveness, ease and low cost of digital surveillance and the effectiveness of threatening negative penalties gives employers little incentive to offer positive rewards to workers, such as job security, promotions and wage increases, to elicit their compliance. This is even more noticeable during economically uncertain times, when workers are afraid of losing employment, and it has also been raised as a cause of recent low wage growth in Australia.[125]

---

118 Finance Sector Union, *Submission 35*, p. 6.

119 Sean Morrison, Victorian Information Comissioner, Office of the Victorian Information Commissioner, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 10.

120 Ibid.

121 See for example, United Workers Union, *Submission 25*, p. 8; Victorian Trades Hall Council, *Submission 28*, p. 10; Australian Nursing and Midwifery Federation, *Submission 38*, p. 5.

122 United Workers Union, *Submission 25*, p. 8; Dr Dale Tweedie, *Transcript of evidence*, p. 15.

123 Australian Services Union, Victorian Private Sector Branch, *Submission 41*, p. 4.

124 Dr Dale Tweedie, Senior Lecturer, Department of Accounting and Corporate Governance, Macquarie University, *Submission 34*, pp. 5–6.

125 Victorian Government, *Submission 43*, p. 18; Macdonald and Heap, *Inquiry into the digital transformation of workplaces*, p. 11.

FINDING 4: Function creep, where surveillance that is deployed for a specific purpose such as safety begins to be used covertly for other reasons such as performance management, is unfair and distressing to employees and poses risks to their privacy and health and safety.

Chapter 3
Impacts of workplace surveillance

Not all workplace surveillance is detrimental to workers, and it can be beneficial, for example, when it protects workers' safety or helps to train staff.[1] However, the general consensus in the evidence presented to the Committee was that surveillance that is intrusive and excessive can negatively affect individual workers, their productivity, workplace culture and workplace relations.

Research into the impacts of workplace surveillance has produced some conflicting results, and this chapter discusses these impacts using the evidence presented to the Committee alongside findings from published studies. What is not in question are the concerns held by individual workers and unions about the use of surveillance in Victorian workplaces, such as the potential harms to workers' health, safety, privacy and rights.

Unease about Victorian employers' use of workplace surveillance is high. To illustrate, the Victorian Private Sector Branch of the Australian Services Union (ASU), which represents workers in the private sector across a range of industries, asked 30 of its union delegates how concerned they were about surveillance in the workplace. Using a scale of 1–10, with 10 being extremely concerned, their average response was 7.4.[2] Figure 3.1 also showcases some of the concerns individual workers have about workplace surveillance in their own words.

This chapter covers the impact of workplace surveillance on productivity, workplace culture, workers' physical and mental health, individual privacy, workers' rights and workplace relations. It concludes by considering how these impacts can be felt more intensely by certain groups of workers.

3.1 There is little evidence to suggest surveillance improves productivity

One area where the research is inconclusive is the impact of workplace surveillance on productivity. Some studies show a positive effect on job motivation whereas other

1 Dr Dale Tweedie, Senior Lecturer, Department of Accounting and Corporate Governance, Macquarie University, *Submission 34*, p. 2; Kirstie Ball, *Electronic monitoring and surveillance in the workplace: literature review and policy recommendations*, Publications Office of the European Union, Luxembourg, 2021, p. 16.

2 Australian Services Union, Victorian Private Sector Branch, *Submission 41*, p. 5.

studies show reduced productivity, and others suggest it has no effect overall.[3] One finding that seems clear is that the relationship between electronic surveillance and performance is positive (that is, productivity goes up with surveillance) when the task being monitored is easy, but it is negative when the task being monitored is complex.[4]

However, there is little evidence overall to support the argument that workplace surveillance improves productivity. For example, a meta-analysis of 94 separate independent studies, which in total sampled 23,461 workers, found there was no evidence that electronic performance monitoring improves employees' performance.[5]

What studies do show is that surveillance can have other impacts on workers that would, at least in theory, make them less productive or even counterproductive. For example, studies show that electronic monitoring creates resentment, decreases job satisfaction, increases stress and strain, and negatively affects employees' wellbeing and work attitudes, which are factors known to reduce productivity.[6] There is also evidence that surveillance can stifle workers' creativity, inhibit discussions with colleagues, lead to self-censorship and result in suboptimal clinical care out of fear that their actions will be monitored and interpreted unfavourably or that they will be questioned about the time they took to complete a task.[7]

Surveys of workers suggest that workplace surveillance does not improve productivity. For example, a 2018 survey of 1,459 people by the Australia Institute's Centre for Future Work found only 37% of respondents agreed that electronic surveillance made workers more efficient and hardworking and 53% disagreed with that statement.[8] A member survey run for this Inquiry by the Victorian and Tasmanian Authorities and Services Branch of the ASU, which represents workers in local government, social and community services, energy, water, transport and public authorities, was even more definitive; only 2% of respondents said electronic surveillance made them more productive, 43% said it made no difference to their productivity, 34% said it made them less productive and 21% said they did not know.[9]

---

3 Thomas Kalischko and René Riedl, 'Electronic performance monitoring in the digital workplace: conceptualization, review of effects and moderators, and future research opportunities', *Frontiers in Psychology*, vol. 12, 2021, p. 7, doi: 10.3389/fpsyg.2021.633031; Kate Morgan and Delaney Nolan, 'How worker surveillance is backfiring on employers', *BBC*, 30 January 2023, <https://www.bbc.com/worklife/article/20230127-how-worker-surveillance-is-backfiring-on-employers> accessed 15 May 2024; Joanna Bronowicka, et al., *'Game that you can't win'?: workplace surveillance in Germany and Poland*, European University Viadrina, Frankfurt, 2020, p. 9.

4 Kalischko and Riedl, 'Electronic performance monitoring in the digital workplace', p. 6.

5 Daniel M. Ravid, et al., 'A meta-analysis of the effects of electronic performance monitoring on work outcomes', *Personnel Psychology*, vol. 76, no. 5, 2023, p. 5.

6 Ibid.; Rudolf Siegel, Cornelius J. König and Veronika Lazar, 'The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behavior: a meta-analysis', *Computers in Human Behavior Reports*, vol. 8, 2022, p. 1, doi: 10.1016/j.chbr.2022.100227; Bronowicka, et al., *'Game that you can't win'?*, p. 9; Australian Human Rights Commission, *Protecting cognition: background paper on human rights and neurotechnology*, Sydney, 2024, p. 35; Australian Manufacturing Workers' Union, *Submission 31*, p. 18; Wilhemina Stracke, Assistant Secretary, Victorian Trades Hall Council, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 32.

7 Bronowicka, et al., *'Game that you can't win'?*, p. 9; Master Electricians Australia, *Submission 11*, p. 5; National Tertiary Education Union, *Submission 24*, p. 8; Libby Muir, Professional Officer, Australian Nursing and Midwifery Federation, Victorian Branch, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 42.

8 Troy Henderson, Tom Swann and Jim Stanford, *Under the employer's eye: electronic monitoring & surveillance in Australian workplaces*, Centre for Future Work, Australia Institute, 2018, pp. 5, 6.

9 Australian Services Union, Victorian and Tasmanian Authorities and Services Branch, *Submission 29*, p. 6.

Figure 3.1 Impact of workplace surveillance on workers

The impact of workplace surveillance on workers: What did the Committee hear?

Mental health

'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

'It gave me such poor mental health I had to leave. Everyone's anxiety was through the roof and it made everyone behave in such a competitive and unhelpful way.'

F, graphic designer

'Workplace surveillance can actually drive employees a bit mad. They become paranoid and stressed. I left my job because I did not want to work in that environment.'

D.C., education worker

Workplace culture

'It just crushes the morale of the employee and in long run the productivity will also suffer. I will never feel happy working for a company that does not trust me and does not value my privacy.'

A, financial services worker

'I don't chat to my colleagues as much … I feel like a naughty child in school. All the morale has disappeared.'

P, retail worker

'[P]rofessional staff at the university all of a sudden in the last couple of years are reporting, 'Well, I'm receiving messages from my manager if I'm not active on Slack every 20 minutes, if I'm not active on Teams every 20 minutes,' … and it is changing the texture of the workplace in a really significant way.'

Dr Jake Goldenfein, University of Melbourne

Work intensity

'I feel like I can't stop for a breather, I'm on my feet all day and even just having a sip of water makes me feel guilty.'

E, hospitality worker

'I feel nervous about stepping away from my computer, and I feel like I have to send unnecessary emails to prove that I'm working.'

S, primary school educator

'The boss was never in the store but would always watch us on the cameras. He would call us and text us 20 minutes into our shift to tell us we weren't doing enough of what he deemed to be our job from watching us through the cameras.'

D, hospitality worker

'We are called when data or sales are 'down' to ask why we aren't selling more … If staff are seen on camera resting or standing in the store, even if everything's been cleaned and put away, it's noted to our manager, and we receive feedback during the week.'

E, retail worker

'Every second of every minute is accounted for. We are given 6 minutes a day outside of breaks to "not be working" — such as stretching, toilet breaks, getting a water or coffee, saying hello to a colleague, taking some time after a bad call. We are considered "late" if we log in to take calls even 5 seconds after our start time.'

K, call centre worker

Sources: Australian Services Union, Victorian and Tasmanian Authorities and Services Branch, *Submission 29*, p. 7; United Workers Union, *Submission 25*, p. 8; Victorian Trades Hall Council, *Submission 28*, pp. 5, 21–3, 29–30, Appendix, p.9; Dr Jake Goldenfein, Senior Lecturer and Chief Investigator of ADM+S Centre (University of Melbourne node), ARC Centre of Excellence for Automated Decision-Making and Society, RMIT, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 51.

Research also shows that workplace surveillance increases the prevalence of counterproductive work behaviours among employees, who act in defiance to get back a sense of control when surveillance makes them feel their employers do not trust them.[10] Counterproductive work behaviours are voluntary behaviours that go against an organisation's standards and goals such as working less, wasting resources or mocking supervisors or colleagues.[11] For example, two studies in the United States found that employees who were closely monitored were more likely to break workplace rules, take more breaks, steal equipment, cheat on tests and work at a slower pace on purpose.[12] Counterproductive work behaviours in response to surveillance were found to be more common in professional roles where workers have more autonomy and more scope to retaliate.[13] Studies also confirm that excessive surveillance often generates the behaviours it was set up to prevent, and this can create a cycle whereby employers escalate workplace surveillance in response.[14]

There are also reports of workers using creative methods to resist surveillance such as installing mouse jigglers, which simulate the movement of a computer mouse, placing a heavy object on keyboard keys to register keystrokes and placing tape over laptop cameras to cover the lens. Others have reversed the surveillance and recorded their employers to prove instances of wage theft or harassment.[15] It can be argued these 'cat and mouse' efforts between employers and employees are unlikely to be increasing productivity and could be counteracting any performance gains achieved from workplace surveillance.[16]

FINDING 5: Research shows that workplace surveillance is unlikely to significantly improve workers' productivity and can produce counterproductive behaviours instead.

Another issue raised in the evidence was the inaccuracy of using workplace surveillance to measure productivity. For example, recording keystrokes and mouse clicks suggests that workers are only productive while on their computer, ignoring activities such as reading document printouts, talking on the phone, helping colleagues

10 Siegel, König and Lazar, 'The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behavior', p. 1; Ball, *Electronic monitoring and surveillance in the workplace*, p. 37; Institute for Public Policy Research, *Watching me, watching you: worker surveillance in the UK after the pandemic*, report prepared by Henry Parkes, London, 2023, pp. 5, 16; Bronowicka, et al., *'Game that you can't win'?*, p. 11; Eurofound, *Employee monitoring and surveillance: the challenges of digitalisation*, Publications Office of the European Union, Luxembourg, 2020, p. 37; Morgan and Nolan, 'How worker surveillance is backfiring on employers'.

11 Siegel, König and Lazar, 'The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behavior', p. 3.

12 Institute for Public Policy Research, *Watching me, watching you*, p. 16; Morgan and Nolan, 'How worker surveillance is backfiring on employers'.

13 Institute for Public Policy Research, *Watching me, watching you*, p. 16.

14 Ball, *Electronic monitoring and surveillance in the workplace*, p. 36; Community and Public Sector Union, Victorian Branch, *Submission 20*, p. 8; Dr Dale Tweedie, *Submission 34*, p. 2.

15 Centre for Decent Work and Industry, QUT, *Submission 13*, p. 8; Ball, *Electronic monitoring and surveillance in the workplace*, p. 20; Institute for Public Policy Research, *Watching me, watching you*, p. 16.

16 Institute for Public Policy Research, *Watching me, watching you*, p. 17; Siegel, König and Lazar, 'The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behavior', p. 9.

at another workstation, taking notes or making calculations on paper.[17] Similarly, using metrics that focus on screentime, physical location and time spent on a task cannot measure work quality or professional judgement, leading managers to place more emphasis on being present or completing tasks quickly rather than producing quality work or providing optimal healthcare or good customer service.[18]

Employers are taking a risk with measuring performance only based on what can be quantified. As Dr Jake Goldenfein, a Senior Lecturer at the University of Melbourne and Chief Investigator at the Australian Research Council Centre of Excellence for Automated Decision-Making and Society, stated:

> If you are doing it in order to really increase throughput in a warehouse, that is one thing, but if you are doing it in ways that just make sure your staff are sitting at their desks and tapping a key every once in a while, then you are not getting productivity.[19]

Tracking activities rather than assessing work quality 'can paradoxically reward less effective workers.'[20] Dr Alysia Blackham, an Associate Professor in law at the University of Melbourne and a member of the National Tertiary Education Union (NTEU), which represents all higher education and university employees in Australia, added that these metrics can create 'perverse incentives' for workers to focus on meaningless tasks. For example, Microsoft Teams sends prompts comparing the number of emails an employee sends with the number sent by their colleagues, even though sending fewer emails is likely to be a sign of greater efficiency.[21]

3.2 Intrusive surveillance can produce a toxic workplace culture

Workplace surveillance that is seen as excessive or intrusive not only has negative effects on employees and little effect on productivity, but it can also undermine the business or organisation that uses it by creating a toxic workplace culture.[22] One meta-analysis of 70 research papers investigating workplace surveillance suggests

---

17 Wendi S. Lazar and Cody Yorke, 'Watched while working: use of monitoring and AI in the workplace increases', *Reuters*, 26 April 2023, <https://www.reuters.com/legal/legalindustry/watched-while-working-use-monitoring-ai-workplace-increases-2023-04-25> accessed 16 May 2024; Associate Professor Alysia Blackham, National Tertiary Education Union, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 48; Professor Peter Holland, Professor, Human Resource Management, School of Business, Law and Entrepreneurship, Swinburne University of Technology, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 2.

18 Chip Cutter and Te-Ping Chen, 'Bosses aren't just tracking when you show up to the office but how long you stay', *The Wall Street Journal Online*, 26 September 2023, <https://www.wsj.com/lifestyle/careers/attention-office-resisters-the-boss-is-counting-badge-swipes-5fa37ff7> accessed 12 June 2024; Institute for Public Policy Research, *Watching me, watching you*, p. 21; Ball, *Electronic monitoring and surveillance in the workplace*, p. 16; Finance Sector Union, *Submission 35*, p. 8; Dr Dale Tweedie, Senior Lecturer, Department of Accounting and Corporate Governance, Macquarie University, public hearing, 26 September 2024, *Transcript of evidence*, p. 12; Alana Ginnivan, Professional Officer, Australian Nursing and Midwifery Federation, Victorian Branch, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 38; Dr Jake Goldenfein, Senior Lecturer and Chief Investigator of ADM+S Centre (University of Melbourne node), ARC Centre of Excellence for Automated Decision-Making and Society, RMIT, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 55.

19 Dr Jake Goldenfein, *Transcript of evidence*, p. 53.

20 Dr Dale Tweedie, *Submission 34*, p. 2.

21 Associate Professor Alysia Blackham, *Transcript of evidence*, p. 49.

22 Victorian Trades Hall Council, *Submission 28*, p. 25.

'there are probably more disadvantages than advantages for organizations when using electronic monitoring.'[23] This section considers the impacts of surveillance on workplace culture, specifically declines in reciprocal trust, job satisfaction and employee commitment.

A common theme in the evidence presented to the Committee was that workplace surveillance leads to declines in trust between employers and employees, especially if employees perceive the purpose of surveillance to be unfair or not transparent.[24] When workplace surveillance is used for performance management, employees can feel that their employer does not trust them, creating resentment and disengagement.[25] For example, the Victorian Trades Hall Council (VTHC), which is the peak body for 40 affiliated Victorian unions, highlighted the following quotes from workers about the impact on organisational culture:

> I have worked in … a vehicle building company that had the values "Respect", "Trust." [They] had extensive surveillance and we had to enter the site with a clear bag only. There were drug sniffer dogs. It was oppressive and felt as though we weren't trusted, or at times, criminals.—S, Autoworker
>
> This does nothing to promote a healthy workplace. This encourages a toxic work environment of distrust and does not bring out the best performance in people. —C, Healthcare Worker
>
> We are here as people and should not be scrutinised unless we are doing something fraudulently.—J, Supermarket Worker[26]

Close surveillance suggests to employees that their manager or employer does not trust their competence, commitment to the organisation, honesty and dependability.[27] Employees also lose trust in their employers, especially if they feel their privacy has been invaded, but studies suggest it is not the surveillance technology itself that workers mistrust but the lack of transparency from employers in how it is or will be used.[28] Employee mistrust can lead to a decline in work performance and increased psychological hazards and staff turnover.[29]

---

23 Siegel, König and Lazar, 'The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behavior', p. 9.

24 See for example, Australian Services Union, Victorian and Tasmanian Authorities and Services Branch, *Submission 29*, p. 4; Australian Manufacturing Workers' Union, S*ubmission 31*, p. 20; Office of the Victorian Information Commissioner, *Submission 39*, p. 8; Professor Peter Holland, *Transcript of evidence*, p. 2; Dr Dale Tweedie, *Transcript of evidence*, p. 13; Institute for Public Policy Research, *Watching me, watching you*, p. 15; Danielle E. Thompson and Adam Molnar, 'Workplace surveillance in Canada: a survey on the adoption and use of employee monitoring applications', *Canadian Review of Sociology*, vol. 60, 2023, p. 805; Bronowicka, et al., *'Game that you can't win'?*, p. 10; Ball, *Electronic monitoring and surveillance in the workplace*, p. 36.

25 Centre for Decent Work and Industry, *Submission 13*, p. 8; Bronowicka, et al., *'Game that you can't win'?*, p. 9.

26 Victorian Trades Hall Council, *Submission 28*, p. 31.

27 Ball, *Electronic monitoring and surveillance in the workplace*, p. 45.

28 Ibid.; Eurofound, *Employee monitoring and surveillance*, p. 40; Kalischko and Riedl, 'Electronic performance monitoring in the digital workplace', p. 6.

29 Australian Nursing and Midwifery Federation, Victorian Branch, *Submission 38*, p. 8.

Workplace surveillance can also result in a culture of fear, where workers are afraid of speaking openly, appearing to be not productive enough or losing their job.[30] And when used for performance management, surveillance can also erode managers' roles and responsibilities. As Dr Goldenfein stated:

> when they [workers] are scared that they are not producing enough they work harder and they work faster and they work in more dangerous ways. And then you [the manager] get to effectively disabuse yourself of the responsibility for the harm that is caused on the basis that, 'Oh, we just set a computational system. The computational system makes the decisions. It wasn't our decision really to tell you you had to work this much.' You even get negative consequences on employers and managers, because their job changes to make them effectively data entry people. They are making sure that the software systems that they have to track their workers are working properly, rather than actually interacting with them on an interpersonal level or necessarily getting to participate in the decision-making that comes out of that data tracking as well.[31]

Workplace culture and performance is strongly linked with employees' job satisfaction, and research indicates that employees who are monitored at work are less satisfied with their job than those who are not.[32] The Victorian Branch of the Community and Public Sector Union (CPSU), which represents workers in the Victorian public service and public authorities and agencies, provided some quotes from workers that showcase this:

> The telematics system makes me feel like my employer fundamentally doesn't trust me to do my job properly without excessive surveillance. This undermines my motivation and morale.[33]

> Going to work is not enjoyable anymore, as you are scrutinised and watched over constantly. Knowing that there is monitoring software installed, whether it is active or not, makes work more stressful. I feel like I have to second-guess everything I do and can't relax and be myself at work.[34]

The effect on job satisfaction can be tempered if employees are able to turn off the surveillance system, if they perceive the surveillance is just, or if their outputs are monitored rather than how they have spent their work hours to achieve those outputs.[35]

Research shows that when surveillance is seen by employees to be excessive, there is lower morale and greater absenteeism and staff turnover.[36] For example, a survey of 7,600 businesses worldwide found that those that planned to implement workplace

---

30 Victorian Trades Hall Council, *Submission 28*, p. 29; Office of the Victorian Information Commissioner, *Submission 39*, p. 8; Dr Jake Goldenfein, *Transcript of evidence*, p. 53; Bronowicka, et al., *'Game that you can't win'?*, p. 10.

31 Dr Jake Goldenfein, *Transcript of evidence*, p. 53.

32 Kalischko and Riedl, 'Electronic performance monitoring in the digital workplace', p. 5; Law Institute of Victoria, *Submission 37*, p. 5.

33 Community and Public Sector Union, *Submission 20*, p. 9.

34 Ibid., p. 11.

35 Kalischko and Riedl, 'Electronic performance monitoring in the digital workplace', p. 6; Ball, *Electronic monitoring and surveillance in the workplace*, p. 54.

36 Eurofound, *Employee monitoring and surveillance*, p. 40; Law Institute of Victoria, *Submission 37*, p. 5.

surveillance during the COVID-19 pandemic were over 80% more likely to report increased staff turnover than those who had no plan to monitor their workforce.[37] Other research shows that the greater the extent of surveillance in a workplace, the less committed employees are to their organisation and the less willing they are to go the extra mile for their employer or colleagues.[38]

FINDING 6: Workplace surveillance that employees see as intrusive and lacking transparency reduces employees' trust in management, job satisfaction and commitment to their organisation, which can result in disengagement, poor workplace culture and increased staff turnover.

3.3 Surveillance intensifies work creating health and safety risks

When employers implement workplace surveillance that tracks task completion or presence at work, it can lead to work intensification where employees work harder and for longer periods of time without any increase in pay.[39] Assistant Secretary at the VTHC, Wilhemina Stracke, gave an example of where workplace surveillance:

> leads to a pressure to perform, a pressure to consistently meet targets. For instance, call centre workers would say to you, 'We get monitored for the number of calls that we take regardless of the complexity of the call. I know that if I'm going to go and have my meeting, my regular catch-up, with the manager, they're going to say, "Well, your call numbers are down, so you need to do better on that."' … So there is this constant pressure, and that worker then feels pressure to keep pushing through and pushing along with things. With work intensification, essentially what surveillance does is it increases the pressure on workers to consistently perform to data targets that are set and that continue to increase because everyone keeps pushing.[40]

While the VTHC is not opposed to increasing efficiencies in the workplace, it disagrees with work intensification that is not linked to improvements in pay or conditions.[41]

Dr Goldenfein from the University of Melbourne explained that in certain workplaces, surveillance that monitors employees' performance rates can have an impact on many employment decisions. In his team's discussions with workers who were originally employed through labour hire arrangements, they heard that workers' work rates determine whether they get given weekend shifts, paid overtime, allocated to work in air-conditioned rooms or offered ongoing or full-time work. These decisions are being

---

37 Institute for Public Policy Research, *Watching me, watching you*, p. 16.

38 Kalischko and Riedl, 'Electronic performance monitoring in the digital workplace', p. 6; Ball, *Electronic monitoring and surveillance in the workplace*, p. 37.

39 National Tertiary Education Union, *Submission 24*, p. 4; Victorian Trades Hall Council, *Submission 28*, p. 20; Building Industry Group of Unions, *Submission 36*, p. 2.

40 Wilhemina Stracke, *Transcript of evidence*, pp. 31–32.

41 Danae Bosler, Assistant Secretary-by-Appointment, Victorian Trades Hall Council, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 32.

made by computational metrics rather than the quality of a person's work or their commitment to the organisation.[42]

The Finance Sector Union (FSU), which represents workers in banking, insurance, superannuation, financial planning and finance, added that when performance targets are set and assessed by artificial intelligence (AI) without any human intervention, this puts even more pressure and stress on staff, especially when their performance rates affect their pay.[43]

Just the expectation of being monitored can place workers under pressure to intensify their workload, and in some industries such as call centres and laundries, task completion rates obtained from surveillance data are displayed for all workers to see.[44] In other cases, workers who know they are being monitored can internalise the expectation that they must always be working at full capacity and can self-discipline and feel guilt and shame in the times they cannot meet that expectation.[45]

This type of surveillance suggests that workers must be productive every moment of the workday, which makes it difficult for them to escape the demands of work.[46] It can contribute to worker stress, which may present as emotional strain, sleep difficulties, depression, anxiety and repetitive stress injuries.[47] It can also create occupational health and safety issues. As Dr Blackham from the NTEU explained:

> In terms of professional work, we are seeing the introduction of keystroke software that monitors how many keystrokes you make every minute, every second, every hour, and how many hours you are at your computer every day. This poses really significant risks of injury …
>
> We are likely to see a growth in occupational injuries if people are expected to remain at a computer continuously for this time. We also have members reporting that they have been told that they are not on Teams long enough, that they need to log into Teams every day to report that they are there, ready for work, then log out so they know when they have gone, or that they are having their bathroom breaks. So their breaks are being monitored. Certainly this is breeding intensification of work.[48]

Another example is warehouse workers who feel so under pressure to meet target pick rates that they forgo bathroom or water breaks and avoid socialising or resting in case they fall behind and are penalised by losing shifts. This can contribute to safety issues

---

42 Dr Jake Goldenfein, *Transcript of evidence*, p. 54.

43 Finance Sector Union, *Submission 35*, p. 10.

44 Victorian Trades Hall Council, *Submission 28*, p. 21; Laundry Association Australia, *Submission 12*, p. 2.

45 Victorian Trades Hall Council, *Submission 28*, p. 22.

46 Dan Nahum and Jim Stanford, Centre for Future Work, Australia Institute, *Technology, standards and democracy*, submission to NSW Legislative Council Select Committee on the Impact of technological and other change on the future of work and workers in New South Wales, 2020, p. 7.

47 Victorian Government, *Submission 43*, p. 18.

48 Associate Professor Alysia Blackham, *Transcript of evidence*, p. 48.

and poorer job satisfaction, health and wellbeing.[49] In some warehouses and factories, workers hold devices or wear wristbands that automatically alert a manager if a worker's productivity falls below 80% of their usual rate.[50] However, as Dr Goldenfein told the Committee, these technologies sometimes fail, creating more pressure on workers:

> What is reported in the research that we did is that these software systems, no matter how sophisticated they are, are always glitchy. The scanner guns run out of batteries, there are dead spots in the warehouse where there is no wi-fi, and the obligation to deal with that glitch is just extra work that the worker will have to do. They will have to prove somehow to the manager, 'It was just recorded wrong because, you know, my scanner ran out of battery.' Some of these workers report having to use multiple apps on their phone consecutively at the same time, and if they log that they have taken a break on one browser tab but not on the other, it records a gap.[51]

Another mechanism for work intensification is the use of gamification in the workplace using surveillance data. Gamification of work occurs when digital surveillance analyses workers' real-time tasks and gives performance scores or time rates that are displayed to all workers. This can place pressure on workers and make them feel they are in constant competition with one another.[52] While gamification can be positive if it is well implemented, promoting engagement, innovation and learning, it can have detrimental effects if it is combined with intrusive surveillance practices or performance management.[53] Not only can the gamification of work create stress and anxiety, it can also increase the risk of accidents in industries where speed is inherently dangerous, such as transport and logistics.[54]

FINDING 7: The pressure of being constantly monitored and tracked at work leads to work intensification, where employees work harder and faster and take fewer breaks, creating occupational health and safety risks.

3.4 Workers' health can be harmed by constant surveillance

Workplace surveillance can have a positive impact on workers' physical and mental health when it acts as a deterrent for occupational violence or aggression, and this can help employees feel safer at work.[55] However, there are situations, especially when the

---

49 Nahum and Stanford, *Technology, standards and democracy*, p. 8; Victorian Trades Hall Council, *VTHC submission to the Inquiry into the digital transformation of workplaces*, submission to House of Representatives Standing Committee on Employment, Education and Training, 2024, p. 17; Dr Jake Goldenfein, *Transcript of evidence*, pp. 54–55.

50 Victorian Trades Hall Council, *VTHC submission to the Inquiry into the digital transformation of workplaces*, p. 17.

51 Dr Jake Goldenfein, *Transcript of evidence*, p. 53.

52 Eurofound, *Employee monitoring and surveillance*, pp. 4, 35.

53 Ibid., p. 35.

54 Dr Dale Tweedie, *Transcript of evidence*, p. 13.

55 Australian Nursing and Midwifery Federation, *Submission 38*, p. 8; Australian Nursing and Midwifery Federation, Victorian Branch, *Hearing notes*, supplementary evidence received 1 November 2024, p. 7.

surveillance is constant or intrusive, that it can be detrimental to workers' physical and mental health. This section discusses these risks and how they manifest.

As mentioned in the previous section, constant workplace surveillance that is linked to performance measures or the time taken to complete tasks can pressure workers to physically exert themselves more by working at a faster pace and taking fewer breaks.[56] Even office workers have reported feeling anxious to leave their desks to fetch water, use the bathroom or take their lunch break in case it could have negative repercussions on their perceived productivity.[57] For example, an entertainment worker told the VTHC:

> I feel like I can't take a break to go to the toilet or have a snack because it is all monitored. If I'm in pain from my disability I hide it because I don't want to seem like I can't do my job.[58]

High levels of stress and exertion and fewer breaks can manifest as physical ailments such as headaches, repetitive strain injury, high blood pressure and musculoskeletal discomfort.[59]

The pressure to work faster and without breaks can also lead to workers cutting corners and taking safety risks, which can contribute to workplace accidents and injuries.[60] Dr Goldenfein provided an example from his research across the warehousing sector where:

> you have people reporting, 'Well, I'm working in a coolroom. I have a little iPad with a countdown clock telling me how much time I have left to finish packing this box, and when it hits zero it goes red, right, and I know I'm in trouble. At the same time I'm a smaller person and I need to grab things off the shelf, but the stairs, the ladders, are all the way down the other end of the room. So I just climb the shelf.'[61]

The Committee also heard that risk taking was a concern for rideshare and delivery riders and drivers where speeding, ignoring road rules or driving when fatigued or in poor weather has resulted in workplace injuries and even fatalities.[62]

---

56 Centre for Decent Work and Industry, *Submission 13*, p. 9; Professor Peter Holland and Dr Jacqueline Meredith, Swinburne University of Technology, *Submission 22*, p. 11; Building Industry Group of Unions, *Submission 36*, p. 3; Eurofound, *Employee monitoring and surveillance*, p. 31.

57 Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 8; Victorian Government, *Submission 43*, p. 15.

58 Victorian Trades Hall Council, *Submission 28*, p. 27.

59 Community and Public Sector Union, *Submission 20*, p. 3; Australian Manufacturing Workers' Union, *Submission 31*, p. 18; Bronowicka, et al., *'Game that you can't win'?*, p. 10; Ball, *Electronic monitoring and surveillance in the workplace*, p. 20; Institute for Public Policy Research, *Watching me, watching you*, p. 15.

60 Community and Public Sector Union, *Submission 20*, p. 11; National Tertiary Education Union, *Submission 24*, p. 5; Dr Fiona Macdonald, Policy Director, Industrial and Social, Centre for Future Work, Australia Institute, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 20; Dr Fiona Macdonald and Dr Lisa Heap, Centre for Future Work, Australia Institute, *Inquiry into the digital transformation of workplaces*, submission to House of Representatives Standing Committee on Employment, Education and Training, 2024, p. 9.

61 Dr Jake Goldenfein, *Transcript of evidence*, p. 51.

62 Centre for Decent Work and Industry, *Submission 13*, p. 10; Sunil Kemppi, Vice President, Employee Representative, Australian Institute of Employment Rights, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 5.

There is strong evidence that workplace surveillance that is inappropriate, poorly designed or linked to disciplinary processes can have a negative impact on employees' mental health such as stress, emotional exhaustion, depression and anxiety.[63] At the same time, if a worker does not know they are being monitored, workplace surveillance may not have any mental health impact.[64] Some studies have been unable to show that electronic performance monitoring has any impact on employee stress, and other studies suggest that the impact depends on a worker's age, with older employees feeling more stressed than younger ones.[65]

However, there is an increased risk to the mental health and wellbeing of workers when they feel they are being constantly watched, such as feeling uncomfortable, frustrated, vulnerable and insecure in the workplace.[66] Sunil Kemppi, Vice President and Employee Representative at the Australian Institute of Employment Rights, a not-for-profit independent organisation that works to promote employment rights, shared that:

> office workers have had annual leave deducted because they sat at a different desk, for example, at the bank that they work for … Knowing that an employer knows where you are at every second of the day has an obvious mental health impact on people.[67]

This type of workplace surveillance can have such a negative impact on employees' mental wellbeing that it can lead to absenteeism and burnout.[68] See Case Study 3.1 for an example. The mental health effects could be even worse for remote workers who already face psychosocial risks linked to working from home such as social isolation, work overload and the pressure to feel they are always seen to be working.[69]

---

63 Bronowicka, et al., *'Game that you can't win'?*, pp. 9–10; Ball, *Electronic monitoring and surveillance in the workplace*, p. 7; Kalischko and Riedl, 'Electronic performance monitoring in the digital workplace', p. 2; Debora Jeske, 'Remote workers' experiences with electronic monitoring during Covid-19: implications and recommendations', *International Journal of Workplace Health Management*, vol. 15, no. 3, 2022, p. 398; Institute for Public Policy Research, *Watching me, watching you*, p. 15; Mena Angela Teebken and Thomas Hess, 'Privacy in a digitised workplace: towards an understanding of employee privacy concerns', *Proceedings of the 54th Hawaii International Conference on System Sciences*, 2021, p. 6668; Siegel, König and Lazar, 'The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behavior', p. 2; Centre for Decent Work and Industry, *Submission 13*, p. 9; Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, pp. 7–8; Victorian Trades Hall Council, *Submission 28*, p. 6; Australian Services Union, Victorian and Tasmanian Authorities and Services Branch, *Submission 29*, p. 7; Australian Manufacturing Workers' Union, *Submission 31*, p. 3; Dr Dale Tweedie, *Submission 34*, p. 2; Victorian Government, *Submission 43*, p. 23; Dr Fiona Macdonald, *Transcript of evidence*, p. 20.

64 Sunil Kemppi, *Transcript of evidence*, p. 5.

65 Kalischko and Riedl, 'Electronic performance monitoring in the digital workplace', p. 5.

66 Eurofound, *Employee monitoring and surveillance*, p. 38; Associate Professor Alysia Blackham, *Transcript of evidence*, p. 38.

67 Sunil Kemppi, *Transcript of evidence*, p. 5.

68 Information Commissioner's Office UK, *Employment practices and data protection: monitoring workers*, October 2023, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers> accessed 14 May 2024; Ball, *Electronic monitoring and surveillance in the workplace*, p. 20; Institute for Public Policy Research, *Watching me, watching you*, p. 5; Jeske, 'Remote workers' experiences with electronic monitoring during Covid-19', p. 403; Australian Lawyers Alliance, *Submission 7*, p. 8; Victorian Farmers Federation, *Submission 16*, p. 2; Community and Public Sector Union, *Submission 20*, p. 12; National Tertiary Education Union, *Submission 24*, p. 5; The Australia Institute Centre for Future Work, *Submission 32*, p. 3; Law Institute of Victoria, *Submission 37*, p. 5; Australian Nursing and Midwifery Federation, *Submission 38*, p. 8; Macdonald and Heap, *Inquiry into the digital transformation of workplaces*, p. 8.

69 Ball, *Electronic monitoring and surveillance in the workplace*, p. 51.

Case Study 3.1 '[T]his is affecting their mental health in really serious ways'

'[W]e recently surveyed more than 500 warehouse distribution centre workers about a new really punitive over-the-top framework that a company has rolled out this year, and what we heard from hundreds and hundreds of workers is that this is affecting their mental health in really serious ways. People are talking about sitting in their car having panic attacks before going to work, being medicated because of the job, it causing marital problems and it causing breakdowns with their relationships with their children, which is really just heartbreaking to hear. And we have had—and I do not say this lightly—members talking about it making them feel suicidal, especially, … cohorts of older men, who may find it hard to access mental health services, or there may be a certain stigma around that or they may feel that if they lose this job they do not have other employment opportunities. It really exacerbates that fear of losing your job. We have a lot of people talking about how dehumanising it is to be monitored second to second, to have their toilet breaks monitored, and just how they feel very resentful and often very ashamed. Sometimes they have worked for an employer for a very long time, and then they are being treated in this fashion in their workplace. And it is having a really big impact on their lives more broadly, not just in the workplace.'

Source: Lauren Kelly, Research and Policy Officer, United Workers Union, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 43.

When employees feel they have little job control due to intrusive or excessive workplace surveillance, it becomes a psychosocial hazard, which is any risk in the workplace that can cause stress and result in psychological or physical harm.[70] As the Victorian Government stated, a psychosocial hazard is 'a serious occupational health and safety issue and can be just as harmful to workers' safety and wellbeing as physical hazards.'[71]

Kat Eather, General Counsel at the Business Council of Australia, which represents over 130 of the nation's leading businesses, agreed that:

> Business does not gain a lot in the long term from having a depressed and run-down and paranoid workforce that believes every moment of their life is being tracked. I do believe that having surveillance to a level [that] is causing psychosocial harm to your staff, that is causing undue stress and anxiety, is already a breach of employers' work health and safety obligations.[72]

Amy Salmon, Principal Psychological Health and Safety Specialist at WorkSafe Victoria, the state's workplace health and safety authority, informed the Committee that under the *Occupational Health and Safety Act 2004* (Vic), 'employers have the

70 Building Industry Group of Unions, *Submission 36*, p. 2.

71 Victorian Government, *Submission 43*, pp. 19–20.

72 Kat Eather, General Counsel, Business Council of Australia, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 20.

obligation to provide and maintain a working environment that is safe and without risks to health. That includes psychological health.'[73]

WorkSafe Victoria's Chief Executive Officer, Joe Calafiore, told the Committee that over the past 20–25 years, there has been a significant increase in workplace mental health injuries in Victoria from around 2–3% to 18%, a trend that is echoed nationwide.[74] Ms Salmon noted that WorkSafe is increasingly recognising that mental health injuries at work regularly stem from high workloads, low job control and a sense of poor organisational justice, which occurs when there is little employer transparency and consultation.[75] As discussed earlier in this chapter, workplace surveillance has been shown to lead to all three of these factors.

FINDING 8: Workplace surveillance that is constant, intrusive or tied to performance measures or disciplinary processes creates stress for employees resulting in poor physical and mental health and can push employees towards taking safety risks that can lead to workplace accidents and injuries.

3.5 Surveillance can breach the privacy of workers and their families

Sean Morrison, the Victorian Information Commissioner, whose office regulates the collection, use and disclosure of personal information in the Victorian public sector, told the Committee that the modern workplace, especially remote working, has created new privacy issues, stating:

> dual SIMs on mobile phones; how employers can access, if it is BYOD, bring your own device, if the employer's software is on there, what monitoring is going on; and requirements for staff to have location services on. Work from home has opened up—we have not got a flood of complaints, but it is going to be the next frontier.[76]

The amount of data employers can collect through workplace surveillance can threaten the privacy of workers and their families. On premises, workplace surveillance can pick up activities at work traditionally considered private, such as the taking of toilet breaks, conversations between colleagues and recording of time spent not 'on task'.[77] Case Study 3.2 provides an example.

---

73 Amy Salmon, Principal Psychological Health and Safety Specialist, WorkSafe Victoria, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 25.

74 Joe Calafiore, Chief Executive Officer, WorkSafe Victoria, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 27.

75 Amy Salmon, *Transcript of evidence*, p. 27.

76 Sean Morrison, Victorian Information Comissioner, Office of the Victorian Information Commissioner, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 13.

77 National Tertiary Education Union, *Submission 24*, pp. 4–5.

Case Study 3.2 '[T]hat is all on camera'

'[T]hey put a camera on a walkway to a toilet. Some of the older women who may be going through menopause or maybe other issues need to go to the toilet and they do not want to be seen going three or four times, or they do not want to be seen coming out and having to go back again. It is not uncommon that people might forget things and they have to go and ask a friend, 'Can I have something?' So that is all on camera, and then they might get asked by their supervisor what they are doing going in and out of the toilet. There might be nothing wrong with that. Sometimes if people are really distressed at work and they need to talk to someone, they will go to a friend, 'Can we go somewhere privately?' There are often not a lot of rooms around in those factories to go, so people will try and step into a private space to do that. In some parts of the workplace it is not appropriate. … [I]n summer people just wear singlet tops and shorts and whatever, so it is really about thinking about where those cameras are placed.'

Source: Jenny Kruschel, National Secretary, Textile Clothing Footwear, Manufacturing Division, Construction, Forestry and Maritime Employees Union, public hearing, Melbourne, 3 September 2024, *Transcript of evidence,* p. 55.

The VTHC added that 'digital workers cannot speak without the employer hearing. Employers monitor the contents of emails, instant messaging apps and other correspondences to a functionally unlimited degree.'[78] Employees can also be monitored in work vehicles and their own homes if they work remotely, which can infringe not only their privacy but also that of anyone else they interact with such as family members or housemates who might be captured on monitoring devices.[79]

For example, a dashboard camera installed in a company vehicle might also have the capability to record audio, and if the camera cannot be switched off it could capture private conversations outside of work hours. Similarly, if employers supply employees with a computer or phone that can be used outside of work hours, employers could have access to employees' physical location, internet search histories and personal data such as their banking details, passwords, medical records and personal correspondence.[80] An example was also given of a *New York Times* writer who found electronic surveillance was capturing private conversations between his family members in the background while he was working from his kitchen during the pandemic.[81]

78 Victorian Trades Hall Council, *Submission 28*, p. 16.

79 Centre for Decent Work and Industry, *Submission 13*, p. 9.

80 Institute of Mercantile Agents, *Submission 14*, p. 4; Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 8; Bronowicka, et al., *'Game that you can't win'?*, p. 10; Information Commissioner's Office UK, *Employment practices and data protection: monitoring workers*.

81 Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 7.

It is often unclear how employers might access the surveillance data at the time it is collected or in the future, and this can have a negative impact on those monitored, such as stress and psychological harm.[82] The collection of sensitive, personal data from surveillance and the use of AI to draw inferences from it in ways that could be inaccurate or discriminatory also has the potential to breach individuals' right to privacy.[83] Studies show that employees have greater privacy concerns when the surveillance is not clearly linked to a stated purpose such as performance and appears to collect data that is unnecessary for business functions.[84]

For example, the CPSU provided quotes from its members who were concerned about surveillance that might capture details of their personal lives, behaviours and activities both inside and outside of work:

> I feel that having my vehicle movements, speed, braking, and location constantly tracked is a massive invasion of my personal privacy. Even when I'm off the clock, I have no way to prevent this monitoring.
>
> ...
>
> I don't feel clear or confident about how AI programs used by the workplace manage personal or sensitive information. I'm concerned about how privacy is managed within the workplace (whereas the focus has been on privacy outside the organisation).
>
> ...
>
> As an employee, I feel this vehicle monitoring system is a major overstep that shows profound disregard for my privacy rights, dignity and autonomy in the workplace. I worry it will irreparably damage morale, trust and the employee-employer relationship.[85]

According to Professor Peter Holland who works in the Human Resource Management Department at Swinburne University of Technology's School of Business, Law and Entrepreneurship, the real concern is when employers do not disclose to their employees the possibility of surveillance outside of work premises. He told the Committee:

> So if you have got your computer open, I think people need to be aware that the conversation is being picked up. Most of the tattleware was put on without people knowing, and they only found out that they were being photographed every 10 seconds or the speed of their keys was being monitored when they got an email saying, 'Where are you? What are you doing?' and they went, 'Where has this come from?' Those companies were not telling people. Again, it is like anything—there are implicit requirements at work of how you act and what you do, but I think with this sort of

---

82 Centre for Decent Work and Industry, *Submission 13*, p. 9; Institute of Mercantile Agents, *Submission 14*, p. 4; Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 9; Eurofound, *Employee monitoring and surveillance*, p. 35.

83 Adjunct Professor Moira Paterson, Castan Centre for Human Rights Law, Faculty of Law, Monash University, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 46.

84 Ball, *Electronic monitoring and surveillance in the workplace*, p. 35.

85 Community and Public Sector Union, *Submission 20*, pp. 7, 8.

> stuff there are no boundaries. The companies can just put it on. They are not breaking any laws. They are saying they are protecting their productivity, their people are not writing inappropriate emails and stuff like that. But it is really work from anywhere; it is workspace not workplace anymore.[86]

Other issues raised by stakeholders was employers' use of private investigators and other investigations when an employee takes sick leave. For example, the Institute of Mercantile Agents, which represents collectors, investigators, process servers and repossession agents throughout Australia, explained how external private investigators working for employers may follow employees to and from their home and watch or record them outside of work hours, which can infringe the privacy of the employees, their families and anyone else in the community who is also in the vicinity and recorded.[87]

Sometimes private investigators are hired to support a cause of action against an employee or to defend a claim against the employer. Other times, they may be hired to determine whether workers are making genuine claims when taking sick leave or seeking workers' compensation. The VTHC and the United Workers Union (UWU), which represents workers across more than 45 industries, gave the example of workers at Coles supermarket cold storage facilities who must complete a form when they return from sick or carers' leave asking them questions about their illness and if they needed prescription medication before they are paid for those hours. Alternatively, workers may receive phone calls from their managers while they are on sick leave, which workers perceive as a form of surveillance.[88]

The VTHC gave another example of warehouse workers at L'Oreal who are asked to 'provide contact details for their personal GP and sign a waiver to allow access to their records before they can return to work' after they have taken sick leave. This practice was introduced into Australian workplaces from the United States where it began.[89] The Australian Manufacturing Workers' Union, which represents workers in all areas of manufacturing such as automotive, food, printing and packaging, also spoke of a sales representative at a multinational car company who was recorded outside his home and at family members' homes while on sick leave following a workplace injury. The worker reported feeling anxious, insulted and violated by this surveillance after finding out when the employer used it as evidence to claim the worker had misrepresented his illness.[90]

Employers' use of neurosurveillance as discussed in Chapter 2 also poses privacy risks for employees because employers are given access to employees' thought patterns, and employees have no discretion or control over what information their employer has

---

86 Professor Peter Holland, *Transcript of evidence*, p. 4.

87 Institute of Mercantile Agents, *Submission 14*, p. 5.

88 Victorian Trades Hall Council, *Submission 28*, pp. 19–20; United Workers Union, *Submission 25*, p. 12.

89 Victorian Trades Hall Council, *Submission 28*, p. 20.

90 Australian Manufacturing Workers' Union, *Submission 31*, p. 14.

access to. This type of monitoring could also expose an employee's feelings and mental health conditions, intruding on their right to mental privacy.[91]

The Committee heard that if employees lose their privacy, it can affect their freedom of speech as well as their ability to authentically participate in the community, which are integral aspects of what it means to be human. When employees feel they are constantly monitored and details of their private lives are accessible to their employer, they may feel as if they are 'never off duty'.[92]

FINDING 9: Workplace surveillance has the potential to impinge on the privacy of workers as well as that of their families and community members who may also be recorded by surveillance devices outside of the workplace, such as in work vehicles or in the home.

3.6 Surveillance can exacerbate the power imbalance in the workplace

Workplace surveillance that is used for purposes beyond safety and security has a risk of collecting large amounts of data that could tip the power imbalance further towards the employer.[93] Not only does surveillance give employers greater visibility of their employees' actions and behaviours, but the data that is gathered is usually only accessible to the employer and not the employees. For example, employers can access and use this data to make decisions about employees including performance ratings and disciplinary action, while employees do not have access to this data to support their own goals, for instance to use it in negotiations or to make a case for promotion. This one-way flow of information places employees in a weaker position compared with employers.[94]

In addition to an imbalance in data access, there is also an inequality of bargaining power between employers and employees when it comes to giving consent to surveillance or opting out. Data and technology business consultant and lawyer Professor Peter Leonard talked about the 'illusion of notice and consent', because this power imbalance calls into question workers' ability to give their genuine consent to surveillance and the only real way of them opting out is to resign.[95] Employees may feel under pressure to consent to surveillance when the alternative may be the loss of employment, or they are fearful of being penalised for expressing their dissent.[96]

---

91 Australian Human Rights Commission, *Protecting cognition*, p. 36; Dr Allan McCay, Academic Fellow, Sydney Law School, University of Sydney, Co-Director, The Sydney Institute of Criminology and President, Institute of Neurotechnology and Law, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, pp. 7–8.

92 Murray Brown, Barrister and Solicitor, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 42; Victorian Trades Hall Council, *Submission 28*, p. 42; Dr Dale Tweedie, *Submission 34*, p. 4; Eurofound, *Employee monitoring and surveillance*, p. 43.

93 United Workers Union, *Submission 25*, p. 4.

94 Institute for Public Policy Research, *Watching me, watching you*, p. 18.

95 Professor Peter Leonard, Principal, Data Synergies and Professor of Practice, UNSW Business School, *Submission 8*, p. 2.

96 Victorian Law Reform Commission, *Workplace privacy: final report*, Melbourne, 2005, p. 35; Eurofound, *Employee monitoring and surveillance*, p. 43.

This is especially pronounced for workers in junior or casual roles or those who have weak bargaining positions, such as retail, call centre or platform workers.[97] The loss of employment can have serious consequences for workers such as financial insecurity, and in difficult economic times, employees would be more reluctant to resign from a job or voice their disapproval of workplace surveillance they have apprehensions about.[98]

Even when workers are asked to agree to a clause in a job contract or a new work policy regarding surveillance or data collection, it is rare they will read the agreement closely before signing or voice their dissent. In other cases, workers may have no choice but to use certain digital applications that also record and share their information and conversations without their knowledge in order to complete their work.[99]

FINDING 10: Workplace surveillance exacerbates the power imbalance between employers and employees by giving employers greater visibility of their employees' actions and behaviours while withholding access to this surveillance data from employees.

FINDING 11: Workers cannot safely opt out or genuinely consent to workplace surveillance if objecting will lead to the loss of employment or possible retaliation from their employer.

3.7 Workers are less likely to take collective action when surveilled

As discussed throughout this chapter, workplace surveillance is changing how employers and employees interact with each other, and this can have a flow-on effect on workplace relations.[100] Workers' freedom to associate and bargain collectively are rights recognised in the International Bill of Human Rights; however, the Committee heard that workplace surveillance can have a chilling effect on workers' discussions with each other and union officials and that employers have used it to identify workers who engage with unions or who push for better conditions in order to intimidate them or disrupt their efforts.[101]

Some examples provided included the use of surveillance to film Woolworths warehouse workers taking industrial action in 2019 as a means of intimidation, a university accessing staff emails and phone calls to NTEU union members and office

97 Dr Dale Tweedie, *Submission 34*, pp. 3–4; Matt O'Connor, Deputy Secretary, Industrial Relations Victoria, Department of Treasury and Finance, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 12.

98 National Tertiary Education Union, *Submission 24*, p. 3; Professor Peter Leonard, Principal, Data Synergies and Professor of Practice, UNSW Business School, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 6.

99 Teebken and Hess, 'Privacy in a digitised workplace', pp. 5–6.

100 Centre for Decent Work and Industry, *Submission 13*, p. 4.

101 United Nations, *International Bill of Human Rights*, <https://www.ohchr.org/en/what-are-human-rights/international-bill-human-rights> accessed 17 December 2024; Construction, Forestry and Maritime Employees Union, Manufacturing Division, *Submission 17*, p. 4; National Tertiary Education Union, *Submission 24*, pp. 7, 22; Eurofound, *Employee monitoring and surveillance*, p. 11; Dr Jean Linis-Dinco, *Submission 6*, p. 1.

bearers, and a Queensland mining company hiring private investigators in 2017 to monitor workers who took industrial action and film them at their homes and out of work hours.[102]

Oscar Kaspi-Crutchett, a researcher at the VTHC, told the Committee that conversations between workers is the first step of any collective bargaining process when a safety or other issue is identified, but these conversations do not occur in a workplace where workers feel all their communication is monitored.[103] This type of surveillance undermines union activity and organising.

Some union officials mentioned the issue of cameras filming or managers overhearing workers' conversations with union officials in lunchrooms where workers 'should be entitled to assume that that is not going to be recorded and used against them.'[104] Another example was the chilling effect of continuous surveillance of farm workers who live in contractor-supplied dormitory arrangements with closed-circuit television (CCTV) cameras and travel to work in contractor-organised transport.[105]

The FSU noted that many of their delegates are concerned that employers are reading their electronic communications relating to union business, which makes it hard for them to have open conversations with their members and prospective members. While the monitoring of such conversations in person would be visible and could be called out, there is no transparency and no law to prevent this from happening through channels such as email or instant messaging.[106] The lack of legal protections is discussed further in Chapter 4.

Kat Hardy, Lead Organiser with the Victorian Private Sector Branch of the ASU, told the Committee that they:

> certainly have examples of employers where if a member has their workplace email as their contact with us, they suddenly stop receiving union communications, and it turns out that, oh, no-one has heard from us in a couple of months unless we have got their personal email.[107]

Nicole McPherson, National Assistant Secretary of the FSU, agreed, saying, 'There are certain employers that are notorious for it.'[108] She added that this results in employees

---

102 National Tertiary Education Union, *Submission 24*, p. 11; United Workers Union, *Submission 25*, p. 9; Victorian Trades Hall Council, *Submission 28*, pp. 6, 8.

103 Oscar Kaspi-Cruchett, Researcher, Victorian Trades Hall Council, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 36.

104 Stephen Fodrocy, Industrial Officer, Australian Manufacturing Workers' Union, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 56; Jenny Kruschel, National Secretary, Textile Clothing Footwear, Manufacturing Division, Construction, Forestry and Maritime Employees Union, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 55.

105 Lauren Kelly, Research and Policy Officer, United Workers Union, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 41.

106 Finance Sector Union, *Submission 35*, p. 6.

107 Kat Hardy, Lead Organiser, Australian Services Union, Victorian Private Sector Branch, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 42.

108 Nicole McPherson, National Assistant Secretary, Finance Sector Union, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 42.

adjusting their behaviour in online chats and emails so they cannot be accused of having views that their employers might disapprove of. This is particularly an issue in the finance sector where many of their members work from home and the only way they can interact with each other is via digital channels. She said:

> Getting them all in a room is not a possibility, so when they have to engage via digital channels and all of the digital channels are monitored all of the time, it has a naturally chilling effect on their ability and their willingness to talk to each other about industrial issues at work.[109]

Researchers overseas have reported that employers have used surveillance technologies to monitor employees' conversations on social media, online forums and private email listservs (email mailing lists), and employers have even attempted to infiltrate these forums to break up union networks.[110] Other ways where surveillance can undermine collective organising and bargaining is when job candidates are profiled to hire those who are considered less likely to be union members.[111]

FINDING 12: The fear of being seen to be talking with union officials or having their communications monitored has a chilling effect on workers' conversations with each other and with union officials, and this undermines collective bargaining efforts.

3.8 The impact of workplace surveillance is worse for some workers

The Committee also heard that the potential harm from workplace surveillance is more pronounced for workers who are marginalised, specifically women, migrants, young people, members of the LGBTIQA+ community or people with disability.[112] These groups are more likely to feel excluded in the workplace and to work in low-paid industries, non-unionised settings or in the gig economy. Workers who have weaker bargaining positions and entitlements are at greater risk of harm from workplace surveillance because they are less able to negotiate its introduction and how the data is used.[113]

The UWU also reminded the Committee that when it comes to surveillance, blue-collar workers experience it differently to white-collar professionals. However, it is the experiences of white-collar workers that are heard more often, such as the impact of

---

109 Ibid.

110 Wilneida Negrón and Aiha Nguyen, 'The long shadow of workplace surveillance', *Stanford Social Innovation Review*, 6 September 2023, <https://ssir.org/articles/entry/the_long_shadow_of_workplace_surveillance> accessed 17 July 2024; Institute for Public Policy Research, *Watching me, watching you*, p. 18.

111 The Centre for Future Work, Australia Institute, *Submission 32*, p. 3.

112 National Tertiary Education Union, *Submission 24*, p. 5; Victorian Trades Hall Council, *Submission 28*, p. 26; Associate Professor Alysia Blackham, *Transcript of evidence*, p. 43; Negrón and Nguyen, 'The long shadow of workplace surveillance'; Ball, *Electronic monitoring and surveillance in the workplace*, p. 8; Institute for Public Policy Research, *Watching me, watching you*, p. 5.

113 Dr Dale Tweedie, *Transcript of evidence*, p. 13; Institute for Public Policy Research, *Watching me, watching you*, p. 19.

digital surveillance on remote workers, and it is their stories that end up shaping public discussions.[114]

Workplaces in precarious industries or with more insecure work are more likely to get away with more intrusive workplace surveillance, which often does not involve very sophisticated technology.[115] The UWU gave the example of industries such as poultry, horticulture and massage therapy that have intrusive surveillance and high levels of control over their workers, who are often migrants, without elaborate technology. Workers are supervised intensely to gain maximum speed and output and their vulnerabilities such as precarious visa and employment arrangements, language barriers, rural isolation and a lack of alternative job options have the potential to be exploited.[116]

The presence of secondary stressors has been shown to multiply the harm of workplace surveillance and create further mental strain on workers. Secondary stressors can include:

- lack of job security or ability to exercise one's rights at work
- lack of consultation mechanisms in the workplace
- autocratic management style and low transparency around decision-making
- limited ability to control the intensity, pace, timing and onset of monitoring
- an already heavy workload or substantial job strain
- lack of clarity around performance measures
- no notice or disclosure about the introduction of workplace surveillance and its purpose.[117]

Also, research suggests some workers are better placed to deal with the emotional labour it takes to navigate surveillance due to their inherent character traits or abilities, such as resilience and flexibility.[118] At the same time, some workers are dealing with other harms to their wellbeing such as stress in their personal life, discrimination, racism, unfair treatment at work or bullying, which place them at greater risk of experiencing the potential harms of workplace surveillance.[119]

Some industries are more likely to use workplace surveillance and AI, which makes their workers more vulnerable. For example, camera surveillance is prevalent in retail settings for security and anti-theft purposes, and retail work is often performed by women, young people and immigrants.[120] Similarly, jobs in retail, sales, customer

---

114 United Workers Union, *Submission 25*, p. 18.

115 Ibid., p. 17; Dr Dale Tweedie, *Submission 34*, p. 6; Ball, *Electronic monitoring and surveillance in the workplace*, p. 27.

116 United Workers Union, *Submission 25*, p. 13; Victorian Trades Hall Council, *Submission 28*, p. 19.

117 Victorian Trades Hall Council, *Submission 28*, p. 26.

118 Dr Dale Tweedie, *Submission 34*, p. 6.

119 Victorian Trades Hall Council, *Submission 28*, p. 27.

120 Ball, *Electronic monitoring and surveillance in the workplace*, p. 27.

service work and bookkeeping are highly susceptible to automation through AI, and these jobs are often held by women and migrant workers.[121] Women are also more likely to work in the service and healthcare industries, which are also highly monitored; however, it must be said that women can find the presence of CCTV cameras reassuring for their safety in certain work environments.[122]

Platform workers, such as those providing rideshare and food delivery services, are also particularly vulnerable to the impacts of workplace surveillance. While they can control when they work, they have no control over the algorithmic surveillance and decision-making that can influence the opportunity of future work.[123] Platform work is short-term, freelance work engaged on a per-task, job or project basis, which is sourced and paid for through a digital platform. The platform algorithms allocate work based on workers' past performance and customer reviews and can also reject payment for substandard work and use this information to determine payment levels and future job offers.[124]

For example, Deliveroo food delivery riders have reported that the platform tracks the average time they take to accept orders, travel to restaurants and deliver to customers, as well as the number of late and unassigned orders. This data is combined with customer reviews to rank workers and determine the jobs they are offered going forward.[125] Platform algorithms can also monitor breaks, discipline workers and deactivate accounts without any right of reply.[126] The Australian Institute of Employment Rights gave the example of a rideshare driver who was expelled from a platform when a customer made a complaint because she was offended by the driver's insistence she wear a mask during the COVID-19 pandemic restrictions.[127]

The use of performance scores based on opaque algorithmic decision-making and unverifiable customer feedback can have a negative impact on workers' wellbeing due to them having no control over the process.[128] By intensely monitoring location and times, platform algorithms can also create safety risks if workers rush, avoid breaks and push themselves too much to boost their performance ratings.[129]

---

121 Victorian Trades Hall Council, *Submission 28*, p. 27.

122 Ibid., p. 31.

123 Dr Dale Tweedie, *Submission 34*, p. 3; Ball, *Electronic monitoring and surveillance in the workplace*, p. 70.

124 Ball, *Electronic monitoring and surveillance in the workplace*, pp. 58–59.

125 Ibid., p. 13.

126 Centre for Decent Work and Industry, *Submission 13*, p. 5; Victorian Trades Hall Council, *Submission 28*, p. 16.

127 Australian Institute of Employment Rights, *Ron McCallum debate: transcript*, supplementary evidence received 2 October 2024, p. 16.

128 Centre for Decent Work and Industry, *Submission 13*, p. 9; James Fleming, Executive Director, Australian Institute of Employment Rights, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 2; Ball, *Electronic monitoring and surveillance in the workplace*, p. 62; Jim Stanford, Director, Centre for Future Work, Australia Institute, *The future of work is what we make it*, submission to Senate Select Committee on the Future of Work and Workers, 2018, p. 21.

129 Dr Dale Tweedie, *Transcript of evidence*, p. 16.

FINDING 13: Workers who are marginalised and have weaker bargaining positions, such as women, young people, migrants, members of the LGBTIQA+ community, people with disability and platform workers, are more likely to experience the harmful impacts of intense workplace surveillance.

Chapter 4
Regulation of workplace surveillance

Victoria's laws have not kept pace with the technological advances and growth of surveillance devices in the workplace. This chapter discusses the areas where Victoria's workplace surveillance laws are failing to safeguard workers' privacy and then examines the effectiveness of regulation interstate, federally and overseas. It goes on to consider Australia's obligations under international conventions and existing best-practice regulation, before concluding with a discussion on how Victoria's laws can be modernised and improved to ensure that surveillance conducted in the workplace is reasonable, necessary and proportionate.

This chapter focuses specifically on the act of workplace surveillance whereas Chapter 5 looks at the privacy and protection of data obtained through workplace surveillance. Throughout both these chapters, the Committee acknowledges that employers have legitimate reasons for workplace surveillance, but at the same time, stronger safeguards are needed to protect the privacy, dignity and autonomy of Victoria's workers as well as their physical and mental safety.

4.1 Workplace surveillance laws in most jurisdictions are inadequate

The technological advances and rapid rise in workplace surveillance discussed in Chapter 2 have outpaced most laws around workplace privacy worldwide.[1] Closer to home, regulation around surveillance and data privacy is inconsistent between Australian jurisdictions and neither state nor federal statutes define what surveillance is, link it back to individuals' right to privacy or set up standards of reasonableness, fairness or proportionality.[2]

As discussed in Chapter 1, New South Wales (NSW) and the Australian Capital Territory (ACT) are the only Australian jurisdictions to have dedicated workplace surveillance laws and the extent to which surveillance laws in other jurisdictions apply to the workplace varies. In addition, existing workplace surveillance laws in Australia rarely cover all forms of surveillance let alone future technologies or contemporary ones such as artificial intelligence (AI) and neurosurveillance.[3]

---

1 Professor Peter Holland and Dr Jacqueline Meredith, Swinburne University of Technology, *Submission 22*, p. 9.

2 Peter Leonard, 'Workplace surveillance and privacy', *Computers and Law: Journal for the Australian and New Zealand Societies for Computers and the Law*, vol. 93, 2021, pp. 63, 67; Australian Manufacturing Workers' Union, *Submission 31*, p. 4.

3 Centre for Decent Work and Industry, QUT, *Submission 13*, p. 11.

Existing surveillance laws in Australia often use a notice and choice framework whereby surveillance is allowed if prior notice is given to the person being surveilled, who can then choose whether to be monitored. However, as discussed in Chapter 3, a real choice is lacking for workers if refusing could mean they are disciplined or lose their employment.[4] General surveillance laws do not acknowledge this power imbalance and only the ACT's workplace surveillance law has a provision for worker consultation.[5] Outside of the public sector and NSW and the ACT, employers' use of workplace surveillance in Australia can proceed largely unimpeded.[6]

This section takes a closer look at how effective the regulation of workplace surveillance is in Victoria, interstate, federally and overseas before considering Australia's obligations under international conventions and best-practice regulation.

4.1.1 Current Victorian workplace surveillance laws are ineffective

As discussed in Chapter 1, Victoria does not have dedicated workplace surveillance laws. Rather, regulation of workplace surveillance is embedded in the *Surveillance Devices Act 1999* (Vic). The other two most applicable laws in Victoria are the *Privacy Act 1988* (Cth) and the *Privacy and Data Protection Act 2014* (Vic); however, both these laws relate to data privacy and neither directly address workplace surveillance (so for this reason they are covered in more detail in the next chapter). Furthermore, they only apply to the public sector and although the Privacy Act also covers businesses with an annual turnover of over $3 million, most Victorian employers do not reach this threshold and are exempt from these two laws.[7] In addition, employee records are exempt from the Privacy Act, which means many instances of workplace surveillance are out of its scope.

Victoria's Surveillance Devices Act was amended in 2006 to prohibit the installation of optical or listening devices in workplace toilets, washrooms, change rooms and lactation rooms. It also bans the tracking of a person's location without their consent and the filming or recording of private activities and conversations in the workplace; however, the way these terms are defined in the legislation means the bans often do not apply in workplace settings, as discussed in more detail below.[8] Other than these provisions, surveillance in Victorian workplaces is largely left unregulated, resulting in an Act that is considered outdated and limited in scope.[9]

---

4 Leonard, 'Workplace surveillance and privacy', p. 67.

5 Centre for Decent Work and Industry, *Submission 13*, p. 11.

6 Murray Brown and Normann Witzleb, 'Big brother at work: workplace surveillance and employee privacy in Australia', *Australian Journal of Labour Law*, vol. 34, no. 3, 2021, p. 28.

7 Australian Bureau of Statistics, *Counts of Australian businesses, including entries and exits*, 2023, <https://www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/jul2019-jun2023> accessed 22 November 2024.

8 Brown and Witzleb, 'Big brother at work', p. 17.

9 Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 10; National Tertiary Education Union, *Submission 24*, pp. 17–18; Law Institute of Victoria, *Submission 37*, p. 3; Victorian Government, *Submission 43*, p. 5; Professor John Howe, Centre for Employment and Labour Relations Law, Melbourne Law School, University of Melbourne, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 1; Adjunct Professor Moira Paterson, Castan Centre for Human Rights Law, Faculty of Law, Monash University, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, pp. 44–45.

Many stakeholders expressed their concerns that Victoria's laws along with existing federal legal frameworks do not adequately, appropriately or directly address workplace surveillance, especially modern surveillance technologies.[10] For example, the Australian HR Institute, the professional body that supports human resources in Australia, polled 74 of its members and found about three in five (59%) of them believe current workplace surveillance and privacy laws do not adequately protect the privacy of workers.[11]

While the consensus in the evidence the Committee received was that Victoria's existing workplace surveillance laws are ineffective at safeguarding employees' privacy, a notable exception was employer groups. They argued that current regulation is adequate and does not need amendment. Both these views are considered in this section; however, the overwhelming evidence from legal experts and academics corroborates the views of individual workers and unions that Victoria's workplace surveillance laws are not fit for purpose.

The specific shortfalls of the Surveillance Devices Act as presented to the Committee are discussed below followed by the views of employer groups.

The definitions of private activities and conversations limit the Act's application

Under the Surveillance Devices Act, it is an offence to install, maintain or use an optical or listening surveillance device to observe, listen to or record a private activity or conversation without the consent of the parties involved.[12] However, the Act's definitions of private activity and conversation result in this rarely applying in a workplace setting.

A private activity is defined as an activity that participants would not want to be seen by others and that occurs in circumstances where the parties would not expect to be observed by someone else. It also does not include activities that take place outside of a building. A private conversation is defined as a conversation in which the parties have a desire to be heard only by themselves and would not expect to be overheard by someone else. In the workplace, there are few activities and conversations that would take place where the participants would expect not to be observed or overheard by others, which restricts the application of these prohibitions and provides limited protection in most workplace settings.[13]

---

10 Australian Lawyers Alliance, *Submission 7*, p. 6; Professor Peter Leonard, Principal, Data Synergies and Professor of Practice, UNSW Business School, *Submission 8*, p. 2; United Workers Union, *Submission 25*, p. 17; Victorian Trades Hall Council, *Submission 28*, p. 5; Australian Nursing and Midwifery Federation, Victorian Branch, *Submission 38*, p. 3; Australian Services Union, Victorian Private Sector Branch, *Submission 41*, p. 4; Victorian Government, *Submission 43*, p. 6; Chris Delaney, Industrial Relations Advisor, Australian Security Industry Association Limited, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 10; Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 44; Associate Professor Alysia Blackham, National Tertiary Education Union, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 39.

11 Australian HR Institute, *Submission 10*, p. 2.

12 *Surveillance Devices Act 1999* (Vic) ss 6, 7.

13 Australian Manufacturing Workers' Union, *Submission 31*, pp. 7–8; Law Institute of Victoria, *Submission 37*, p. 3; Victorian Government, *Submission 43*, p. 6; Peter Johnson, Compliance and Regulatory Affairs Advisor, Australian Security Industry Association Limited, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 9; Adjunct Professor Moira Paterson, *Transcript of evidence*, pp. 44–45.

The Committee also heard that this means that the surveillance of private activities or conversations that take place in areas where employers have informed workers that surveillance devices are installed would be allowed.[14] Also, legal experts added that the definitions are vague and could be interpreted in different ways. For example, it is unclear if a voicemail message played aloud on speaker is considered a private conversation, and if employees working from home should expect activities occurring in their home to be private even though they may have consented to being monitored while at work.[15]

The definition of a tracking device is outdated rendering most protections void

Similarly, the Surveillance Devices Act's definition of a tracking device means that tracking the location of an employee using a modern surveillance device will often not constitute an offence under the Act. The Act makes it an offence to install, maintain or use a tracking device to monitor a person's geographical location without the person's express or implied consent.[16] However, under the Act a tracking device is an electronic device of which the primary purpose is determining the geographical location of a person or object. This would exclude multifunctional devices with tracking abilities such as mobile phones, laptops and other modern devices where Global Positioning System (GPS) tracking capabilities are but one of their secondary features.[17] This means that employers could use these multifunctional devices to track employees' location without seeking consent.[18] Furthermore, using tracking devices is not prohibited if another individual owns the property to which the tracking device is fitted, so tracking devices fitted to employer-supplied devices or vehicles may not be covered under the Act.[19]

It is unclear how the Act regards devices with multiple surveillance functions

Stakeholders also mentioned that there is uncertainty around how the Act treats devices with multiple surveillance functions, such as cameras that are used to record both image and sound and wearable devices that have optical, tracking and data surveillance capabilities.[20]

---

14 National Tertiary Education Union, *Submission 24*, pp. 17–18.

15 Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 10; Law Institute of Victoria, *Submission 37*, p. 3.

16 *Surveillance Devices Act 1999* (Vic) s 8.

17 Australian Workers' Union, *Submission 27*, pp. 2–3; Victorian Government, *Submission 43*, p. 6; Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 45; Danae Fleetwood, Master of Philosophy research student, Centre for Decent Work and Industry, QUT, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 22; Australian Law Reform Commission, *Serious invasions of privacy in the digital era: final report*, Australian Government, Sydney, 2014, p. 283.

18 Australian Workers' Union, *Submission 27*, pp. 2–3.

19 Victorian Government, *Submission 43*, p. 6.

20 Australian Security Industry Association Limited, *Submission 21*, p. 3; Danae Fleetwood, *Transcript of evidence*, p. 22.

The Act only regulates data surveillance by law enforcement officers

The Surveillance Devices Act directly addresses data surveillance only in terms of its use by law enforcement officers. This means that Victorian employers monitoring their workers' emails, computer and internet usage do not fall within the scope of the Act.[21] Considering data surveillance is currently one of the most common forms of workplace surveillance, this narrow treatment shows how Victoria's workplace surveillance laws need updating.[22]

The Act's notion of consent ignores the workplace power imbalance

The Surveillance Devices Act requires the express or implied consent of the person being monitored through optical, listening or tracking devices.[23] In the workplace, implied consent could be deemed given if an employee signs an employment contract with a clause stating awareness of and consent to surveillance or confirms receipt of a workplace surveillance or employee monitoring policy in induction documentation. It can also be deemed granted when an employer issues a notice to all employees when implementing a relevant policy and no objections are made.

However, as discussed in Chapter 3, this approach fails to recognise the imbalance of power in employment relationships, and that workers may choose to work under surveillance because to do otherwise might mean disciplinary action or dismissal.[24] This is most pronounced for workers who have relatively weak bargaining positions such as casual workers, platform workers and those with poor union representation.[25]

The Committee also heard that the inclusion of catch-all surveillance clauses in employment contracts and general or vague sentences about workplace surveillance in workplace policies provide little detail resulting in employees giving implied consent without a clear understanding of how their employer will use surveillance devices in the workplace.[26]

There is no obligation to notify or consult with employees

Stakeholders also raised that the Surveillance Devices Act does not require employers to notify employees of surveillance conducted in the workplace apart from the limited requirements as discussed above to obtain consent for GPS tracking and recording

---

21 National Tertiary Education Union, *Submission 24*, p. 18; Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 45.

22 Australian Manufacturing Workers' Union, *Submission 31*, p. 9; Professor Peter Leonard, Principal, Data Synergies and Professor of Practice, UNSW Business School, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 6.

23 *Surveillance Devices Act 1999* (Vic) ss 6, 7, 8.

24 National Tertiary Education Union, *Submission 24*, p. 18; Australian Manufacturing Workers' Union, *Submission 31*, p. 8; Law Institute of Victoria, *Submission 37*, p. 3; Australian Services Union, Victorian Private Sector Branch, *Submission 41*, p. 11; Victorian Government, *Submission 43*, p. 6.

25 Dr Dale Tweedie, Senior Lecturer, Department of Accounting and Corporate Governance, Macquarie University, *Submission 34*, pp. 3–4.

26 Australian Services Union, Victorian Private Sector Branch, *Submission 41*, p. 12; Susan Accary, President, Victoria Branch Committee, Australian Lawyers Alliance, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, pp. 28–29; Dr Jacqueline Meredith, Lecturer, Swinburne Law School, Swinburne University of Technology, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 4.

private activities and conversations.[27] Victorian employers who use surveillance are not required to have a workplace surveillance policy, nor must they tell workers the exact nature of how they will conduct surveillance and how they will use the information obtained.[28] There is also no requirement for employers to consult with affected employees or unions or to assess the reasonableness and invasiveness of the surveillance methods they use.[29]

Employer groups argue that current surveillance laws are effective

Employer groups disagreed with the view that Victoria's workplace surveillance laws are inadequate or ineffective. They argued that the Surveillance Devices Act provides Victorian employees with enough protection and its scope is broad enough to cover technological advancements, especially when considered together with occupational health and safety (OHS) laws and the Commonwealth Privacy Act.[30] However, they did not provide evidence to refute the above arguments about the Surveillance Devices Act's shortcomings or the fact that the Privacy Act does not apply to all Victorian workplaces, and exempts small businesses and employee records.

The Institute of Mercantile Agents, which represents collectors, investigators, process servers and repossession agents throughout Australia, acknowledged that while it seemed existing laws provide satisfactory protection to those being monitored, there was scope for requiring employers to notify and adequately explain to their employees how and why they are conducting workplace surveillance and how they will use the associated information.[31]

Business groups, namely the Business Council of Australia (BCA), the Australian Industry (Ai) Group and the Victorian Chamber of Commerce and Industry (Victorian Chamber), argued that the Victorian Government should hold off on considering any changes to workplace surveillance legislation until Commonwealth reforms to the Privacy Act are announced. They said only then will the full landscape around surveillance and data privacy regulation be clear, and consequently, any need to update Victorian legislation may disappear.[32] The Victorian Chamber added that time was needed to see how recent federal legislative changes regarding workers' right to disconnect have affected the working environment before making any further changes.[33]

---

27 National Tertiary Education Union, *Submission 24*, p. 19; Australian Nursing and Midwifery Federation, *Submission 38*, p. 3; Australian Services Union, Victorian Private Sector Branch, *Submission 41*, p. 12; Susan Accary, *Transcript of evidence*, p. 25.

28 National Tertiary Education Union, *Submission 24*, p. 19; Australian Services Union, Victorian Private Sector Branch, *Submission 41*, p. 12.

29 National Tertiary Education Union, *Submission 24*, pp. 19–20; Leonard, 'Workplace surveillance and privacy', p. 62.

30 Master Electricians Australia, *Submission 11*, p. 1; Institute of Mercantile Agents, *Submission 14*, p. 3; Victorian Automobile Chamber of Commerce, *Submission 26*, pp. 8–9; Australian Industry Group, *Submission 40*, pp. 3, 14–15; Amelia Bitsis, Executive Director, Policy and Advocacy, Victorian Chamber of Commerce and Industry, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 15.

31 Institute of Mercantile Agents, *Submission 14*, p. 3.

32 Scott Barklamb, Principal Advisor, Workplace Relations Policy, Australian Industry Group, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 35; Kat Eather, General Counsel, Business Council of Australia, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 18; Amelia Bitsis, *Transcript of evidence*, p. 16.

33 Victorian Chamber of Commerce and Industry, *Submission 18*, p. 3.

While the first tranche of amendments to the Privacy Act were passed in November 2024, none dealt with workplace surveillance. Also, changes to the small business and employee records exemptions and the treatment of biometric data and geolocation tracking—which the Attorney-General's Department proposed in its 2023 review of the Privacy Act and which were supported by the Australian Government—were not included.[34] It is unlikely that any further amendments will be made to the Privacy Act before the 2025 federal election. See Chapter 5 for further discussion of these amendments and their potential impact on workplace surveillance regulation.

The Ai Group and the Victorian Chamber added that if the Committee concluded that the regulation of workplace surveillance in Victoria needs updating, it should limit any changes to the creation of best-practice guidelines developed in conjunction with unions and employers because guidelines can be flexible, rapidly introduced and responsive to new technologies or workplace practices.[35] The Victorian Chamber also suggested that enterprise agreements might be a more appropriate avenue for regulating workplace surveillance.[36] While the Committee heard of instances where workplace surveillance clauses have been introduced to enterprise agreements to establish safeguards for employee privacy, it also heard that these were rare with one study of nine Australian industries finding that only about 4% of enterprise agreements include such clauses.[37] Furthermore, such collectively bargained solutions are only likely to be reached in industries with heavy union presence.[38]

FINDING 14: Victoria's workplace surveillance laws are ineffective and in need of updating because they do not cover all scenarios or technologies and do not require employers to notify or consult with their employees about surveillance in the workplace.

4.1.2 Workplace surveillance laws in NSW and ACT are better but also have failings

NSW and the ACT have the country's most comprehensive workplace surveillance laws, and while they provide greater protection to workers than Victoria's laws, they still have some weaknesses and are in need of updating. Both the *Workplace Surveillance Act 2005* (NSW) and the *Workplace Privacy Act 2011* (ACT) require employers to

---

34 Kat Eather, *Transcript of evidence*, p. 18; Matt O'Connor, Deputy Secretary, Industrial Relations Victoria, Department of Treasury and Finance, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 7.

35 Australian Industry Group, *Submission 40*, p. 4; Scott Barklamb, *Transcript of evidence*, p. 36; Yoness Blackmore, Principal Advisor, Workplace Relations Policy, Australian Industry Group, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 37; Victorian Chamber of Commerce and Industry, *Submission 18*, p. 3.

36 Victorian Chamber of Commerce and Industry, *Submission 18*, p. 3.

37 Building Industry Group of Unions, *Submission 36*, pp. 7–8; Nicole McPherson, National Assistant Secretary, Finance Sector Union, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 45; Brown and Witzleb, 'Big brother at work', p. 12; Alysia Blackham, 'Surveillance, data collection and privacy at work: a new application of equitable organisations?', *Australian Journal of Labour Law*, (forthcoming), 2025, p. 10; Professor John Howe, *Transcript of evidence*, p. 3.

38 Alysia Blackham, 'Setting the framework for accountability for algorithmic discrimination at work', *Melbourne University Law Review*, vol. 47, no. 63, 2023, p. 95; Brown and Witzleb, 'Big brother at work', p. 12; Lauren Kelly, Research and Policy Officer, United Workers Union, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 44.

develop and adhere to a workplace surveillance policy and provide employees at least 14 days' notice before surveillance begins (except for new employees so long as they are informed before they start employment). The notice must include details of:

- the type of surveillance that will be used
- how the surveillance will be carried out
- when the surveillance will begin
- whether the surveillance will be intermittent or continuous.[39]

The ACT also requires employers to specify in the notice who the ordinary subject of surveillance will be, the purpose for which the employer may use or disclose the information obtained from the surveillance, and that the worker may consult with the employer about how the surveillance will be carried out. Both laws require employers to have all cameras visible, notices in the workplace where cameras are operating and on vehicles that will be tracked, as well as computer monitoring policies.[40]

If an employer wishes to use workplace surveillance in performance appraisals, then employers must notify employees of this in advance, and if an employer wants to be able to discipline or dismiss a worker based on information uncovered through data surveillance, then this potential consequence must be stated in the employer's computer monitoring policy.[41] In the ACT, employers must give workers access to surveillance records about them upon request; if they refuse, employers cannot use these records in legal proceedings or to take adverse action against the worker.[42]

Employers in both jurisdictions are prohibited from conducting covert surveillance unless they have obtained a court order based on an employee's suspected unlawful activity. In granting the court order, the Magistrate must consider the impact on the employee's privacy and in the ACT specifically, whether there are more appropriate ways of collecting relevant information than using covert surveillance and whether it is more appropriate for the matter to be referred to law enforcement. If such a court order is granted in either jurisdiction, a surveillance supervisor must be appointed, the order cannot be issued for longer than 30 days and it may be cancelled by the Magistrate on the Magistrate's own initiative or on application from the worker, employer or other affected person. In the ACT, the surveillance supervisor must be independent of the employer.[43]

---

39 Leonard, 'Workplace surveillance and privacy', pp. 70–71; Aaron Magner and Steven Penning, 'Workplace surveillance and privacy', *Commercial Law Quarterly*, vol. 20, September–November, 2006, p. 28; Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 12.

40 Leonard, 'Workplace surveillance and privacy', pp. 70–71.

41 Magner and Penning, 'Workplace surveillance and privacy', pp. 26, 28.

42 *Workplace Privacy Act 2011* (ACT) s 23; Victorian Trades Hall Council, *Submission 28*, p. 34.

43 *Workplace Privacy Act 2011* (ACT) ss 28, 29, 30, 33; *Workplace Surveillance Act 2005* (NSW) ss 25, 27, 29, 31; Magner and Penning, 'Workplace surveillance and privacy', pp. 27–28; Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 12; Victorian Trades Hall Council, *Submission 28*, p. 34.

The NSW Workplace Surveillance Act covers optical, data and tracking surveillance, whereas listening surveillance falls under the *Surveillance Devices Act 2007* (NSW). Similarly, the ACT Workplace Privacy Act covers optical, data and tracking surveillance, and listening surveillance is covered by the *Listening Devices Act 1992* (ACT).[44] The latter Act allows for covert surveillance using a listening device if it is to protect an employer's lawful interests.[45] NSW only allows workplace surveillance when the employee is at work (which can mean either in or outside of the workplace) whereas the ACT states it is only allowed in the workplace; however, data surveillance is allowed outside of work if an employee is using employer-provided equipment, and in the ACT if the tracking function in a tracking device cannot be deactivated.[46] Failure to comply with either the NSW or ACT laws may amount to a criminal offence. Table 4.1 compares workplace surveillance regulation in the ACT, NSW and Victoria.

Table 4.1 Comparison of workplace surveillance legislation in the ACT, NSW and Victoria

Provision	ACT	NSW	Victoria
Ban of workplace surveillance in toilets, washrooms and change rooms	✓	✓	✓
Ban of workplace surveillance in lactation rooms	✓		✓
Ban of workplace surveillance in parent rooms	✓		
Ban of workplace surveillance in prayer rooms	✓		
Ban of workplace surveillance in first-aid rooms and sick bays	✓		
Ban on blocking websites or email delivery relating to industrial matters	✓	✓	
Written notice of surveillance	✓	✓	
Visible notice of camera surveillance and visible cameras	✓	✓	
Visible notice of tracking devices in vehicles	✓	✓	
Disclosure of how surveillance will be conducted and type of device used	✓	✓	
Disclosure of when surveillance will commence	✓	✓	
Disclosure of whether the surveillance will be intermittent or continuous	✓	✓	
Disclosure of whether surveillance will be for a specified period or ongoing	✓	✓	
Disclosure of who is the ordinary subject of surveillance	✓		
Disclosure of the purpose of surveillance	✓		
Employers must consult with workers about the conduct of surveillance	✓		
Independent surveillance supervisor appointed for covert surveillance	✓		
Employers must provide workers with access to surveillance data held about them upon request	✓		

Sources: Adapted from Victorian Trades Hall Council, *Submission 28*, p. 45; *Workplace Privacy Act 2011* (ACT); *Workplace Surveillance Act 2005* (NSW); *Surveillance Devices Act 1999* (Vic).

44 Leonard, 'Workplace surveillance and privacy', pp. 71–72.

45 John Wilson and Kieran Pender, 'The rights and wrongs of workplace surveillance', *Ethos: Law Society of the ACT Journal*, no. 267, 2023, p. 25.

46 Leonard, 'Workplace surveillance and privacy', pp. 71–72; Magner and Penning, 'Workplace surveillance and privacy', p. 27.

Stakeholders noted that Victorian workers are not afforded the protections provided in workplace surveillance laws in the ACT and NSW, such as notice, disclosure and consultation requirements, the right to access their surveillance data, and strict limits on covert surveillance.[47] The ACT workplace surveillance law was considered more robust and more clearly drafted than the NSW law.[48]

Despite suggesting that Victoria replicate these provisions, stakeholders also felt that the NSW and ACT laws were outdated, inadequate at safeguarding workers' privacy and should not be used as a best-practice model.[49] For example, Swinburne University noted that so long as employers notify their workers of workplace surveillance, they are effectively free to overtly monitor their employees in whatever way they choose. While the ACT allows for consultation with workers, workers in NSW have no mechanism to challenge or negotiate how the surveillance is conducted.[50] As Swinburne Law School lecturer Dr Jacqueline Meredith stated:

> while the [NSW and ACT] approach to covert surveillance is beneficial, when we look at overt surveillance or open surveillance, there are really no limitations. So the approach in those other jurisdictions is really not that much better than the current approach in Victoria for overt or open surveillance. There are no restrictions. The employer does not have to have a legitimate purpose. They do not have to do the surveillance by the least intrusive means possible. As long as there is notice and disclosure, that is going to be sufficient.[51]

The Victorian Private Sector Branch of the Australian Services Union (ASU), which represents workers in the private sector across a range of industries, added that both Acts have exemptions for 'surveillance by agreement' whereby surveillance is allowed if workers or their representative union agree to it. This effectively allows employers in the ACT and NSW to insert general surveillance clauses in employment contracts to meet their requirements.[52] Another concern was whether the definitions of 'at work' in the NSW Act and 'in a workplace' in the ACT legislation unambiguously cover flexible working arrangements, especially working from home.[53]

In 2022, a NSW Legislative Council Select Committee on the impact of technological and other change on the future of work and workers in NSW, which considered whether the state's workplace surveillance laws were fit for purpose in the twenty-first century, also found that the legislation needed updating to take into account the fairness of workplace surveillance, new and emerging technologies and the changing nature of work.[54]

---

47 Victorian Trades Hall Council, *Submission 28*, p. 32; Law Institute of Victoria, *Submission 37*, p. 7.

48 Chris Molnar, Co-Chair, LIV Workplace Relations Committee, Law Institute of Victoria, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, pp. 24–25; Dr Jacqueline Meredith, *Transcript of evidence*, p. 3.

49 Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 45.

50 Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 13; Magner and Penning, 'Workplace surveillance and privacy', p. 24.

51 Dr Jacqueline Meredith, *Transcript of evidence*, p. 5.

52 Australian Services Union, Victorian Private Sector Branch, *Submission 41*, p. 12.

53 Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 13.

54 Parliament of New South Wales, Legislative Council Select Committee on the Impact of Technological and Other Change on the Future of Work and Workers in New South Wales, *Impact of technological and other change on the future of work and workers in New South Wales: final report—workplace surveillance and automation*, November 2022, pp. 23–25.

FINDING 15: While workplace surveillance laws in New South Wales and the Australian Capital Territory provide workers with more protections than Victorian legislation, they should not be considered best-practice examples because they do not cover all technologies and scenarios and nor do they require workplace surveillance to be reasonable, necessary and proportionate.

The Committee also heard that surveillance legislation in the other Australian states and territory are inconsistent, outdated, poorly understood and in some cases poorly drafted. Due to the lack of dedicated workplace surveillance laws in Queensland, Western Australia, South Australia, Tasmania and the Northern Territory, employers must comply with general privacy and surveillance laws.[55]

In 2014, the Australian Law Reform Commission undertook a review of surveillance legislation across Australia and found inconsistencies in the types of surveillance that are covered, what types of surveillance are considered an offence, and the defences and exceptions that apply in each jurisdiction. It concluded that ultimately the legal rights of individuals and the legal obligations of individuals or organisations using surveillance 'are highly contingent upon their location.'[56]

Data and technology business consultant and lawyer Professor Peter Leonard noted that there has not been any substantial improvement in the decade since. He added that Australia's surveillance statutes were developed to address older and more limited technologies and circumstances that did not include working from home and employer-provided devices. He said these statutes are difficult to interpret, their overlap with privacy legislation is often misunderstood, and even lawyers disagree on which legal standards should apply when determining safeguards for workplace surveillance.[57]

4.1.3 Federal laws do not specifically cover workplace surveillance

Federal laws do not specifically touch on workplace surveillance as discussed earlier, so therefore they provide limited protections for workers. This section discusses relevant federal laws and how they deal with workplace surveillance, if at all.

Federal laws relating to surveillance devices do not clearly extend to the workplace

As mentioned in Chapter 1, the *Telecommunications (Interception and Access) Act 1979* (Cth) covers the covert interception of communications over a telecommunications system by a third party. While this would suggest that an employer must notify

55 Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 10; Leonard, 'Workplace surveillance and privacy', pp. 69, 70.

56 Australian Law Reform Commission, *Serious invasions of privacy in the digital era*, pp. 278–280; Leonard, 'Workplace surveillance and privacy', pp. 69–70.

57 Professor Peter Leonard, *Submission 8*, pp. 2–3; Principal Professor Peter Leonard, Data Synergies and Professor of Practice, UNSW Business School, *Submission 8, Attachment 1*, p. 1.

workers if it will conduct surveillance over its telecommunications systems, another interpretation is that an employer would not classify as a third party if it recorded workplace conversations.[58]

The Attorney-General's Department is also currently reviewing Australia's electronic surveillance legislative framework with the aim of making it technology neutral, so it can apply to whatever way surveillance is conducted. However, at this stage it is unclear whether these reforms will extend to workplace surveillance as the Department noted states and territories are the primary regulators of surveillance devices.[59]

The Fair Work Act provides limited protection around surveillance

Most industrial relations matters in Victoria are now governed by the *Fair Work Act 2009* (Cth).[60] However, the Fair Work Act does not specifically refer to workplace surveillance or provide workers with much privacy protection.[61] The Fair Work Act allows employers to collect and maintain employee records, which hold personal information to enable payment of wages and compliance with workplace laws, but there are no specific provisions to protect the privacy of this information.[62]

One area where the Fair Work Act somewhat protects employees in relation to workplace surveillance is that it prohibits employers taking adverse action or acting on information gathered using surveillance if it discriminates against a worker on various grounds such as race, gender, sexual preference, marital status, pregnancy, breastfeeding, age, disability, religion, political opinion, national extraction or social origin.[63]

The Fair Work Act also requires enterprise agreements to oblige employers to consult with employees about a major workplace change that is likely to have a significant effect on employees. However, the definition of significant effect includes termination; changes in workforce composition, operation or size; changes in required skills; elimination or reduction of job opportunities or tenure; changes to work hours; need for retraining or relocation; and job restructure. As such, it is unclear if the introduction of workplace surveillance would be considered a major workplace change under the Fair Work Act.[64]

To date, the Fair Work Commission, which is Australia's workplace tribunal, has justified workplace surveillance if the employer complies with relevant state or territory legislation and the surveillance is proven to be for a legitimate purpose. However, the

---

58 Brown and Witzleb, 'Big brother at work', p. 11.

59 Victorian Government, *Submission 43*, p. 9.

60 Ibid., p. 5.

61 Brown and Witzleb, 'Big brother at work', p. 12; Lisa Heap, *No blood—no job: Australia's privacy laws and workers' rights*, Centre for Future Work, Australia Institute, 2024, p. 11.

62 Heap, *No blood—no job*, p. 11.

63 Centre for Decent Work and Industry, *Submission 13*, p. 12; Australian Manufacturing Workers' Union, *Submission 31*, pp. 9, 11; Brown and Witzleb, 'Big brother at work', p. 13.

64 Australian Manufacturing Workers' Union, *Submission 31*, p. 10; Victorian Government, *Submission 43*, p. 7.

Commission has upheld the dismissal of employees based on covert or out-of-hours surveillance if the employee's actions were unlawful or could cause serious harm to the business.[65]

The Privacy Act has many gaps in terms of workplace privacy

As mentioned in previous sections, the *Privacy Act 1988* (Cth) does not specifically cover workplace surveillance and the Office of the Australian Information Commissioner, which regulates compliance with the Privacy Act, states that employers conducting surveillance must follow relevant state and territory laws.[66] Furthermore, the Privacy Act only covers the public sector and employers with an annual turnover of over $3 million. Since over 90% of Australian employers are considered small businesses and do not meet this threshold, most private sector employers are exempt from complying with the Privacy Act.[67]

Another exemption is employee records. The Privacy Act allows employers to collect and use workers' personal information if it is reasonably necessary for, or is directly related to, the employer's functions and the employment relationship. This can include information to enable the payment of wages and determination of benefits, but the definition is broad enough to include information about employee productivity and performance.[68]

As mentioned in Section 4.1.1, the Attorney-General's Department, in its 2023 review of the Privacy Act, recommended the enhancement of privacy protections for private sector employees. Proposed reforms to the Privacy Act suggested that the small business exemption and employee records exemption would be removed, but these reforms are yet to materialise, and it remains uncertain whether they would extend to information gathered through surveillance.[69]

FINDING 16: Federal laws such as the *Fair Work Act 2009* (Cth) and *Privacy Act 1988* (Cth) do not specifically refer to workplace surveillance and there are gaps in the types of records and employers they cover, which provides workers limited privacy protection.

4.1.4 Workplace surveillance laws overseas offer varying levels of protection

As in Australia, workplace surveillance laws overseas vary between jurisdictions and offer different levels of protection. Some are more effective than others, but none stand out as ideal practice. Technological advancements in surveillance generally

65 Professor Peter Leonard, *Submission 8, Attachment 1*, pp. 5–6; Brown and Witzleb, 'Big brother at work', p. 12; Blackham, 'Surveillance, data collection and privacy at work', p. 6.

66 Leonard, 'Workplace surveillance and privacy', p. 9.

67 Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 44.

68 Australian Nursing and Midwifery Federation, *Submission 38*, p. 3; Victorian Government, *Submission 43*, p. 8.

69 Victorian Government, *Submission 43*, pp. 8–9; Brown and Witzleb, 'Big brother at work', p. 11; Professor John Howe, *Transcript of evidence*, p. 1.

have outpaced the law in many countries creating gaps such as few if any protections around digital and biometric surveillance. However, some countries have introduced relatively strong regulation.[70] Table 4.2 provides examples of overseas workplace surveillance regulation.

Table 4.2 Examples of workplace surveillance regulation overseas

Jurisdiction	Workplace surveillance regulation
Austria	• Any surveillance that may affect workers' dignity must be co-determined with works councils (bodies of employee representatives within a single workplace) or through individual agreements with employees.
Belgium	• National collective bargaining agreements regulate video and data surveillance.
Canada	• In some provinces, adverse action against a worker is prohibited if the worker does not consent to measures that contravene their right to privacy or data protection.
Croatia	• Consultation with works councils is mandatory when employers implement new technology at work or changes to the organisation of work.
Cyprus	• Commissioner for Personal Data Protection publishes guidelines for employers on data and biometric surveillance.
Finland	• Closed-circuit television (CCTV) and GPS tracking surveillance must be co-determined with works councils.
France	• Employers must consult with works councils when they seek to introduce new technology that might affect working conditions. • Employers must justify the purpose of biometric surveillance and explain why the use of more standard measures is insufficient. • National Data Protection Authority publishes guidance on surveillance for employers.
Germany	• CCTV and GPS tracking surveillance must be co-determined with works councils.
Greece	• Hellenic Data Protection Authority publishes guidelines on data, video, GPS tracking and biometric surveillance.
Iceland	• Data surveillance must include a visual notice identifying the surveillance controller.
Italy	• Monitoring of employees using audiovisual surveillance is generally prohibited. If employers wish to use it, they must provide commercial justification for its use and obtain consent from the relevant union. • The national labour authority oversees dispute resolution.
Netherlands	• Works councils must consent to adoption, amendment or withdrawal of data privacy and workplace surveillance policies.
Norway	• Digital monitoring or surveillance of individuals requires a licence from the national data inspectorate and must have a legitimate purpose. • In some workplaces, CCTV cannot be used to monitor employee activity. • Employers must consult with unions about workplace surveillance design, implementation and control measure evaluation.
Portugal	• Processing of employees' biometric data is only permitted for monitoring attendance and controlling access to work premises. • Remote surveillance is only permitted for the purpose of protecting workers, clients and property, and cannot be used to monitor employees' performance.

70 Australian Manufacturing Workers' Union, *Submission 31*, p. 22; Australian Nursing and Midwifery Federation, *Submission 38*, p. 10.

Jurisdiction	Workplace surveillance regulation
Spain	• Employees have a right to privacy when using employer-supplied digital devices. • Employers must establish standards around the use of digital surveillance devices. • Surveillance is prohibited in areas of the workplace where work is not conducted, such as lunchrooms.
Sweden	• Employers must negotiate with trade unions about any significant workplace changes including the introduction of digital surveillance.
United Kingdom (UK)	• UK Information Commissioner publishes guidelines on employee data protection and monitoring. The Code is not legally binding but is used in proceedings where there is an alleged breach of the UK *Data Protection Act 2018*. • The Employment Rights Bill introduced to the UK Parliament in October 2024 does not address workplace surveillance.
United States of America	• The federal *Electronic Communications Privacy Act of 1986* does not cover all types of surveillance and has limited applicability to workplace surveillance; however, it does require employers to have a business reason for data surveillance. • Statutory protections vary markedly between states. • In Connecticut, Delaware and New York, employers must notify employees of any surveillance practices. • In California, private sector employers with an annual turnover over $25 million must protect the privacy of employee records, and operators of large distribution centres must disclose performance quotas and expected outputs to their employees.

Sources: Eurofound, *Employee monitoring and surveillance: the challenges of digitalisation*, Publications Office of the European Union, Luxembourg, 2020, pp. 16–18; UK Government, *Factsheet: Employment Rights Bill overview*, (n.d.), <https://assets.publishing.service.gov.uk/media/6752f32a14973821ce2a6cc2/employment-rights-bill-overview.pdf> accessed 14 January 2025; Victorian Trades Hall Council, *Submission 28*, p. 36; Australian Manufacturing Workers' Union, *Submission 31*, p. 22; Australian Nursing and Midwifery Federation, *Submission 38*, p. 10; Victorian Government, *Submission 43*, p. 11; State of California Department of Justice, *California Consumer Privacy Act (CCPA)*, 2024, <https://oag.ca.gov/privacy/ccpa> accessed 20 May 2024.

4.1.5 There are no international conventions specifically on workplace surveillance

Australia has no obligations under international conventions around the surveillance of employees in the workplace because there is no internationally recognised convention specific to workplace surveillance or the protection of employee data that is legally binding.[71] However, there are international conventions around the right to privacy and freedom of association that Australia has ratified.

Article 12 of the Universal Declaration of Human Rights and Article 17(1) of the International Covenant on Civil and Political Rights recognise individuals' right not to have their privacy arbitrarily or unlawfully interfered with, but this protection is primarily focused on personal and private life, so it is unclear whether it could be relied upon to protect privacy in the workplace.[72] An individual's right to freedom of association is recognised by Article 23 of the Universal Declaration of Human Rights, Article 8 of the International Covenant on Economic, Social and Cultural Rights, and

71 Australian Industry Group, *Submission 40*, p. 27; Victorian Government, *Submission 43*, p. 9.

72 United Nations, *Universal Declaration of Human Rights*, 1948, <https://www.un.org/en/about-us/universal-declaration-of-human-rights> accessed 15 January 2025; United Nations, *International Covenant on Civil and Political Rights*, 1966, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> accessed 15 January 2025; Victorian Government, *Submission 43*, pp. 9–10; Australian Lawyers Alliance, *Submission 7*, p. 11.

Article 22 of the International Covenant on Civil and Political Rights.[73] This right could be threatened by intrusive workplace surveillance, as discussed in Chapter 3.

In terms of workplace surveillance, the International Labour Organization (ILO) has a non-binding Code of Practice on the Protection of Workers' Personal Data.[74] The ILO is an agency of the United Nations that brings together governments, employers and workers of member states to set labour standards promoting social justice and internationally recognised human and labour rights. Its code of practice, published in 1997, provides guidance around workplace surveillance but it has no binding force and does not impose any legal obligations.[75]

This code of practice sets out standards for employee monitoring including:

- workers' right to be informed in advance of surveillance including the technologies used along with the reason for surveillance and when it will occur
- limiting the use of continuous monitoring to health and safety purposes or the protection of property
- restricting covert monitoring for when employers suspect criminal activity
- requiring employers to consider the potential consequences of monitoring on workers' individual and collective rights.[76]

The code of practice is informed by a number of principles including proportionality, whereby employers are obliged to use the least intrusive means of surveillance to achieve a reasonable objective.[77] The other principles include legitimacy, where data collected through surveillance is only used for reasons directly related to the worker's employment, purpose limitation, which requires that surveillance data is only used for the purposes for which it was originally collected, and transparency, where workers are informed of the data collection process, the rules around collection, and their rights.[78]

FINDING 17: Australia has no obligations under international conventions to regulate or prohibit the surveillance of workers because there are no legally binding international conventions directly related to workplace surveillance.

---

73 United Nations, *Universal Declaration of Human Rights*; United Nations, *International Covenant on Economic, Social and Cultural Rights*, 1966, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights> accessed 15 January 2025; United Nations, *International Covenant on Civil and Political Rights*; Eurofound, *Employee monitoring and surveillance: the challenges of digitalisation*, Publications Office of the European Union, Luxembourg, 2020, p. 7; National Tertiary Education Union, *Submission 24*, p. 22.

74 International Labour Organization, *Protection of Workers' Personal Data: an ILO code of practice*, International Labour Office, Geneva, 1997.

75 Australian Industry Group, *Submission 40*, p. 28; Victorian Government, *Submission 43*, p. 9.

76 Eurofound, *Employee monitoring and surveillance*, p. 7; Australian Lawyers Alliance, *Submission 7*, p. 11; Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, pp. 10–11; Australian Nursing and Midwifery Federation, *Submission 38*, p. 9.

77 Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, pp. 10–11.

78 Construction, Forestry and Maritime Employees Union, Manufacturing Division, *Submission 17*, p. 5.

4.1.6 There are several principles that should guide best-practice regulation

Since there are gaps in the regulation of workplace surveillance in most jurisdictions, it is difficult to identify examples of best practice to satisfy this part of the terms of reference. However, the Committee came across examples of best-practice principles that have been adopted in a range of workplace surveillance settings that Victoria could learn from. Some of these principles have been discussed already, such as advance notification to workers, clear and easy to understand workplace surveillance policies and consultation with workers. The Australian HR Institute also notes that best practice in workplace surveillance involves employers assessing the need for conducting surveillance and clearly defining its purpose.[79] See Case Study 4.1 for an example of good practice at the Office of the Victorian Information Commissioner (OVIC), which regulates the collection, use and disclosure of personal information in the Victorian public sector.

Case Study 4.1 'We introduced that policy to the staff very carefully'

'[W]e actually run CCTV in our own workplace. We do that because … we hold, as the information regulator, an enormous volume of highly sensitive material, be it cabinet documents, be it privacy cases. We also hold a lot of Victoria Police data because we regulate Victoria Police. For that reason we felt that it was very important to know whether there were circumstances in which that data might be exposed. So we run CCTV cameras; we have prominent signage. We introduced that policy to the staff very carefully, and we have a very tight access control regime. It can only be accessed by two people in concert—never a single person; that is inappropriate access—and only in response to an identified incident. For example, we had a building worker who managed to … set off an alarm and they were wandering around the premises. We wanted to see what they had looked at. We were able to review the footage and see that they had not in fact been exposed to anything sensitive. That was the full extent of the access. We would never access that material for other purposes. We may need to adjust our policy to take account of, for example, if there was a workplace injury. But when we introduced the policy, we did not include that in our use policy. So these are the sorts of things you then need to evolve and talk to your staff about. This is a high-management overhead, so to employers who are thinking that this is a nice Swiss army knife to solve a lot of workplace problems: no, it actually creates a very big overhead for you if you want to be compliant with the Privacy Act consistently. And when you have got new people being onboarded you have to go through that all over again. I think those are big considerations. So it is not as attractive as it sounds.'

Source: Rachel Dixon, Privacy and Data Protection Deputy Commissioner, Office of the Victorian Information Commissioner, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, pp. 12–13.

79 Australian HR Institute, *Submission 10*, p. 4.

The UK Information Commissioner's Office (ICO) produces guidance on data protection and monitoring workers, and this provides another example of best-practice principles for workplace surveillance. The ICO is a public entity that upholds information rights in the public interest and promotes openness by public bodies and data privacy for individuals. Its guidance on monitoring workers is primarily for employers to give them greater certainty around relevant regulation and to protect workers' data protection rights.[80]

The guidance highlights to employers the need to balance their business interests with workers' rights and freedoms under data protection law, which in the UK is the *Data Protection Act 2018* and the *UK General Data Protection Regulation 2021* (discussed in more detail in Chapter 5). It reminds employers to be clear about the purpose for using surveillance and to select the least intrusive means to achieve it, noting that there are higher expectations of privacy in the home than in the workplace when monitoring people who work from home.[81]

Under UK data protection law, employers must identify a lawful basis to process workplace surveillance data. There are six lawful bases:

- consent: worker freely gives consent to processing, which in the employment context is usually not appropriate due to the power imbalance
- contract: processing is required for an employment contract with a worker, which is an unlikely scenario
- legal obligation: processing is necessary for the employer to comply with the law
- vital interests: processing is needed to protect someone's life, which generally applies to matters of life and death and would therefore be rare in the workplace
- public task: processing is necessary to perform a task in the public interest or for the employer's official functions
- legitimate interests: processing is necessary for employers' legitimate interests or those of a third party, unless workers' rights override them.[82]

The legitimate interests basis can be broken down into three key tests: purpose (is there a legitimate interest?), necessity (is surveillance needed to achieve that purpose?) and balance (is the legitimate interest overridden by workers' interests, rights or freedoms?).[83]

The ICO recommends employers undertake a data protection impact assessment (DPIA) to identify the most appropriate basis for employee monitoring. Completing a DPIA helps employers to identify and minimise the risks of surveillance and offers

---

80 Information Commissioner's Office UK, *Employment practices and data protection: monitoring workers*, October 2023, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers> accessed 14 May 2024.

81 Ibid.

82 Ibid.

83 Ibid.

an avenue for employers to consult with workers about the proposed surveillance.[84] Under the principles described above, it may be difficult for employers to justify the use of keystroke monitoring, screenshot capture and always-on webcams, especially for employees working from home.[85]

The ICO also highlights the concepts of fairness, transparency and data minimisation, whereby employees should only be monitored in ways they would reasonably expect and that would not unduly adversely affect them, employers clearly explain to workers how their information will be collected and processed, and employers do not collect more information than they need to achieve their purpose. There are additional conditions employers need to meet if they are collecting highly sensitive data such as biometric data.[86]

Another set of principles for workplace surveillance proposed in the literature focus on procedural, distributive and informational justice. Procedural justice refers to employees' ability to express their views and challenge surveillance; distributive justice refers to the fairness of outcomes based on surveillance; and informational justice refers to giving employees clear and timely explanations of any surveillance that affects them.[87]

FINDING 18: Best-practice regulation of workplace surveillance incorporates the principles of reasonableness, necessity, proportionality, fairness, transparency and data minimisation.

4.2 Victoria's workplace surveillance laws need modernising

Workplace surveillance is increasingly presenting risks to individuals' privacy and evidence presented throughout this Inquiry overwhelmingly pointed to the need for law reform in Victoria.[88] This situation is not unique to Victoria—every law reform body that has reviewed surveillance and privacy laws around the nation in recent years has recommended significant reforms to adequately deal with current and emerging surveillance methods.[89]

---

84 Ibid.

85 Institute for Public Policy Research, *Watching me, watching you: worker surveillance in the UK after the pandemic*, report prepared by Henry Parkes, London, 2023, p. 23.

86 Information Commissioner's Office UK, *Employment practices and data protection: monitoring workers*.

87 Kirstie Ball, *Electronic monitoring and surveillance in the workplace: literature review and policy recommendations*, Publications Office of the European Union, Luxembourg, 2021, p. 74.

88 For example, Australian Manufacturing Workers' Union, *Submission 31*, p. 4; The Australia Institute Centre for Future Work, *Submission 32*, p. 4; Finance Sector Union, *Submission 35*, p. 4; Dr Jacqueline Meredith, *Transcript of evidence*, p. 2; Wilhemina Stracke, Assistant Secretary, Victorian Trades Hall Council, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 29; Chris Molnar, *Transcript of evidence*, p. 24; Professor John Howe, *Transcript of evidence*, p. 3; Danae Fleetwood, *Transcript of evidence*, p. 20; Sean Morrison, Victorian Information Comissioner, Office of the Victorian Information Commissioner, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 10; Associate Professor Alysia Blackham, *Transcript of evidence*, p. 47.

89 Professor Peter Leonard, *Submission 8, Attachment 1*, p. 2.

Unions noted that workplace surveillance is left largely unregulated in Victoria and that the situation has reached a 'crisis point' with the growing use of surveillance, lack of transparency, popularity of remote working and advances in technology.[90] As Lauren Kelly, Research and Policy Officer at the United Workers Union, which represents workers across more than 45 industries, stated:

> it is not as simple as saying to the employer, 'You're not allowed to do this.' Actually, the conversation becomes, 'You are allowed to do this, but you probably shouldn't.' That is a much more difficult campaign to run, and it means that rather than appealing to our industrial power, which is what we should be able to do as unions, we are often in a position where we have to run a public narrative campaign and say, 'Well, you can do this, but you shouldn't, and it's going to look bad for you if you do and it'll look bad to the public and it'll look bad to shareholders.' That is not what unions should be spending our time doing.[91]

Unions also stressed that workplace surveillance provisions rarely make it into enterprise agreements except in a few industries where there is strong union presence. This makes it even more important to introduce legislation so that all Victorian workers are protected.[92]

The Committee heard that law reform should balance employers' legitimate needs for workplace surveillance with protecting employees' privacy, acknowledge the power imbalance between employees and employers, go beyond relying on express or implied consent, and be based on principles of reasonableness and proportionality.[93] At the very least, employees should be notified of surveillance and consulted about it.[94]

Suggested approaches to law reform ranged from new legislation to a state code of practice to educational guidelines.[95] While employer groups suggested the Committee hold off on recommending legislative changes until there was clarity around federal reforms, legal academics suggested that workplace surveillance law reform in Victoria is important and urgent and should not be delayed in the hope that federal reforms remove exemptions for small businesses and employee records or that national harmonisation of workplace surveillance laws, which may take years, occurs, to obviate its need.[96]

---

90 Finance Sector Union, *Submission 35*, p. 4; Wilhemina Stracke, *Transcript of evidence*, p. 30.

91 Lauren Kelly, *Transcript of evidence*, p. 39.

92 Associate Professor Alysia Blackham, *Transcript of evidence*, p. 45; Sarah Roberts, Victorian Division, Secretary, National Tertiary Education Union, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 45; Alana Ginnivan, Professional Officer, Australian Nursing and Midwifery Federation, Victorian Branch, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 40; Dan Nahum, *Working from home, or living at work?: hours of work, unpaid overtime, and working arrangements through COVID-19*, Centre for Future Work, Australia Institute, 2021, p. 45.

93 Professor Peter Leonard, *Submission 8, Attachment 1*, p. 2; Dr Dale Tweedie, *Submission 34*, p. 7; Dr Jacqueline Meredith, *Transcript of evidence*, p. 2; Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 45; Associate Professor Alysia Blackham, *Transcript of evidence*, p. 39.

94 Professor John Howe, *Transcript of evidence*, p. 4; Chris Molnar, *Transcript of evidence*, p. 24; Matt O'Connor, *Transcript of evidence*, p. 3; Dr Jake Goldenfein, Senior Lecturer and Chief Investigator of ADM+S Centre (University of Melbourne node), ARC Centre of Excellence for Automated Decision-Making and Society, RMIT, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 52.

95 Professor John Howe, *Transcript of evidence*, p. 4; Australian Industry Group, *Submission 40*, p. 25.

96 Professor John Howe, *Transcript of evidence*, p. 3; Associate Professor Alysia Blackham, *Transcript of evidence*, p. 47; Dr Fiona Macdonald, Policy Director, Industrial and Social, Centre for Future Work, Australia Institute, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, pp. 19, 22.

This section discusses how Victoria's workplace surveillance laws could be modernised by covering the state's power to regulate in terms of how Victorian laws interact with federal laws, the types of legal protections Victoria could introduce and how these changes might impact businesses. The chapter concludes by considering how to protect workers who are surveilled at work by third parties who are not authorised to undertake this surveillance.

4.2.1 The Fair Work Act preserves Victoria's power to regulate workplace surveillance

As mentioned earlier, Victoria has referred most of its industrial relations power to the Commonwealth, which means that the Fair Work Act governs industrial relations matters in Victoria unless federal legislation expressly preserves the state's power to regulate a particular matter. Workplace surveillance is one such matter; Section 27(2)(m) of the Fair Work Act lists workplace surveillance as a matter that state law may deal with, and therefore the Act preserves Victoria's power to regulate workplace surveillance.[97]

Previous reports by the Victorian and New South Wales law reform commissions have acknowledged that while national laws regulating workplace surveillance would be ideal, states should not avoid legislating in this area. They argued that existing laws are not strong enough and the pursuit for clarity and national harmonisation should not occur at the expense of comprehensive regulation.[98]

FINDING 19: Victoria has the power to regulate workplace surveillance under Section 27(2)(m) of the *Fair Work Act 2009* (Cth).

4.2.2 Safeguards around workplace surveillance must be enhanced

Victoria needs more protections around workplace surveillance because currently there are few safeguards around its use and workers are often unaware of why the surveillance is taking place, whether it is necessary, and how the information is going to be used.[99] As has been discussed throughout this report, basing regulation on consent is inadequate for workplace surveillance if employees feel they have no other option but to agree. At the same time, employers may also be disadvantaged if workers refuse to consent to surveillance that may be reasonable. According to OVIC, a better solution is to base workplace surveillance laws on Victorians' right to privacy and balancing that with employers' legitimate needs for using surveillance.[100]

---

97 *Fair Work Act 2009* (Cth) s 27(2)(m); Victorian Government, *Submission 43*, p. 5.

98 Victorian Law Reform Commission, *Workplace privacy: final report*, Melbourne, 2005, p. 20.

99 Karen Batt, Secretary, Community and Public Sector Union, Victorian Branch, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 39.

100 Office of the Victorian Information Commissioner, *Submission 39A*, p. 8.

This section considers the types of reforms suggested by stakeholders in the evidence before recommending changes to Victoria's workplace surveillance laws that are technology neutral, amenable to future national harmonisation and balance the needs of employers with workers' right to privacy.

The Committee heard a number of suggestions for law reform

While most of the evidence supported the use of workplace surveillance for legitimate purposes, the following suggestions for law reform were presented to the Committee to enhance protections for workers:

- banning workplace surveillance when workers are not at work, including a ban on social media trawling[101]
- in terms of surveillance, defining 'workplace' as wherever work is being performed, so as to include the home and defining 'workers' broadly to cover non-traditional categories of employees[102]
- requiring employers to demonstrate a genuine need for workplace surveillance and that the surveillance is proportionate to meeting that need[103]
- requiring employers to notify employees about any surveillance, including the type, timing, limitations and visibility of surveillance devices[104]
- obligating employers to consult with their workers before implementing changes to workplace surveillance[105]
- obligating employers to share surveillance data upon request by an employee or the employee's legal representative[106]
- requiring employers to have a workplace surveillance policy[107]
- requiring visible signage in all company vehicles with GPS tracking capabilities[108]
- classifying excessive or inappropriate workplace surveillance as a psychosocial hazard and making greater use of existing OHS regulation[109]

---

101 Australian Lawyers Alliance, *Submission 7*, p. 7; Community and Public Sector Union, Victorian Branch, *Submission 20*, p. 12; Australian Services Union, Victorian Private Sector Branch, *Submission 41*, p. 6.

102 Centre for Decent Work and Industry, *Submission 13*, p. 11; National Tertiary Education Union, *Submission 24*, p. 21; Chris Molnar, *Transcript of evidence*, p. 26; Wilhemina Stracke, *Transcript of evidence*, p. 33.

103 Community and Public Sector Union, *Submission 20*, p. 12; National Tertiary Education Union, *Submission 24*, p. 24.

104 Australian Lawyers Alliance, *Submission 7*, p. 7; National Tertiary Education Union, *Submission 24*, p. 22; Australian Workers' Union, *Submission 27*, p. 4.

105 Community and Public Sector Union, *Submission 20*, p. 12; Australian Workers' Union, *Submission 27*, p. 4; Australian Nursing and Midwifery Federation, *Submission 38*, p. 12.

106 Australian Lawyers Alliance, *Submission 7*, p. 9; National Tertiary Education Union, *Submission 24*, p. 22; Australian Workers' Union, *Submission 27*, p. 4.

107 Australian Lawyers Alliance, *Submission 7*, p. 7.

108 Ibid.

109 Law Institute of Victoria, *Submission 37*, p. 2; Professor John Howe, *Transcript of evidence*, p. 2.

- prohibiting invasive monitoring practices unless they are expressly justified[110]
- prohibiting covert surveillance unless a formal order is issued by a court or tribunal[111]
- prohibiting the use of surveillance evidence in disciplinary procedures[112]
- banning the use of surveillance devices in meal or break rooms, at times and locations where union officials have exercised their right of entry under the Fair Work Act and when workers are engaged in protected industrial action[113]
- giving employees the right to opt out of surveillance[114]
- introducing an independent regulator for workplace surveillance[115]
- establishing adequate penalties or fines for non-compliance with workplace surveillance laws[116]
- developing new workplace surveillance laws that reflect modern surveillance techniques[117]
- ensuring information that has been incidentally collected through workplace surveillance (such as surveillance in the home or from body-worn cameras or bring-your-own devices) is not stored[118]
- implementing similar workplace surveillance laws to those in NSW and the ACT.[119]

The National Tertiary Education Union (NTEU), which represents all higher education and university employees in Australia, mentioned most of these suggestions but instead framed them around six workplace privacy principles to guide the development of a new workplace surveillance statute. These principles, which were drawn from the ILO declarations and conventions relating to freedom of association and collective bargaining, are comprehensiveness; transparency; freedom of association; legitimate purpose and proportionality; governance and accountability; and effective compliance and enforcement.[120]

The Victorian Trades Hall Council (VTHC), which is the peak body for 40 affiliated Victorian unions, also covered most of these suggestions when it proposed that Victoria introduce a Privacy in Working Life Act, which would protect workers from intrusive workplace surveillance and sit separately from the Surveillance Devices

---

110 Australian Lawyers Alliance, *Submission 7*, p. 7.

111 Ibid.; National Tertiary Education Union, *Submission 24*, p. 22.

112 Australian Nursing and Midwifery Federation, *Submission 38*, p. 12.

113 Construction, Forestry and Maritime Employees Union, Manufacturing Division, *Submission 17*, p. 6; National Tertiary Education Union, *Submission 24*, p. 23.

114 Australian Workers' Union, *Submission 27*, p. 4.

115 Australian Nursing and Midwifery Federation, *Submission 38*, p. 13; National Tertiary Education Union, *Submission 24*, p. 25.

116 Australian Lawyers Alliance, *Submission 7*, p. 9; National Tertiary Education Union, *Submission 24*, p. 25.

117 Australian Lawyers Alliance, *Submission 7*, p. 7.

118 Office of the Victorian Information Commissioner, *Submission 39*, p. 9.

119 Law Institute of Victoria, *Submission 37*, p. 1; Business Council of Australia, *Submission 5*, p. 1.

120 National Tertiary Education Union, *Submission 24*, p. 20.

Act.[121] This proposed legislation was also supported by other union submissions.[122] The VTHC also called for prohibiting employers from taking adverse actions on workers based on surveillance information, banning surveillance in non-work areas and outside of working hours, limiting workplace surveillance to security and safety purposes, allowing workers to opt out of surveillance that threatens their health and safety, banning covert surveillance unless authorised by a magistrate or police warrant, and mandating notice, disclosure and consultation requirements when introducing or expanding workplace surveillance.[123]

VTHC also suggested recognising the psychosocial harms of workplace surveillance and that unions work with WorkSafe Victoria, the state's workplace health and safety authority, to develop a guide on the use and risks of workplace surveillance. In terms of data, it suggested protecting workers' sensitive personal data and the privacy of their communications, banning the undisclosed resale of workers' personal data and giving workers access to their surveillance data. Regarding compliance and enforcement, it called for fines for employers who violate workplace surveillance and privacy laws, civil remedies for workers who have experienced abusive surveillance practices or had their personal data mishandled, and that unions and Wage Inspectorate Victoria, an independent regulator of certain state employment laws, have powers to investigate alleged breaches.[124]

OVIC suggested that the Committee consider whether Victoria should develop a new principles-based framework for regulating workplace surveillance. It originally proposed that it be a separate regulatory mechanism to the Victorian Privacy and Data Protection Act, but at a public hearing, Victoria's Information Commissioner, Sean Morrison, suggested that it could be merged with Victoria's current privacy framework so as not to have two competing sets of privacy obligations for the public sector.[125]

However, not everyone agreed that regulating workplace surveillance through data protection was the correct way forward.[126] For example, Dr Alysia Blackham, an Associate Professor in law at the University of Melbourne and a member of the NTEU, said:

> this is much bigger than just data protection. Really, we need to be thinking about substantive limits on when employers can or should surveil their workforce and in particular that that should be for a legitimate purpose and that it should be proportionate to that purpose.[127]

---

121 Victorian Trades Hall Council, *Submission 28*, p. 8.

122 Australian Workers' Union, *Submission 27*, pp. 3–5; Australian Services Union, Victorian and Tasmanian Authorities and Services Branch, *Submission 29*, p. 9; Finance Sector Union, *Submission 35*, p. 11; Building Industry Group of Unions, *Submission 36*, p. 8; Australian Services Union, Victorian Private Sector Branch, *Submission 41*, p. 5; Australian Education Union, Victorian Branch, *Submission 42*, p. 1.

123 Victorian Trades Hall Council, *Submission 28*, pp. 43–44.

124 Ibid.

125 Office of the Victorian Information Commissioner, *Submission 39*, p. 10; Sean Morrison, *Transcript of evidence*, p. 10.

126 National Tertiary Education Union, *Submission 24*, pp. 15–16.

127 Associate Professor Alysia Blackham, *Transcript of evidence*, p. 39.

Similarly, Dr Jake Goldenfein, a Senior Lecturer at the University of Melbourne and Chief Investigator at the Australian Research Council Centre of Excellence for Automated Decision-Making and Society, stated:

> data protection is not the ideal way in which to manage this. Data protection gives rights to individuals to consent to certain kinds of data processing and to know what kind of data is stored about them. But if you really want to manage surveillance and data governance in a workplace, it cannot be just at the individual level …
>
> An individual cannot really understand how these systems are used in a workplace just by exercising rights given to them under data protection, and that is why we are seeing more holistic things happen in other parts of the world, like duties to consult … That is absolutely baseline. Same with transparency—it should be absolutely baseline.[128]

Another common theme in the evidence was the need for workplace surveillance legislation to be technology neutral. This would future proof regulation so it can apply to any advances in this rapidly evolving area of technology.[129] Stakeholders suggested that regulation move away from specific types of surveillance devices to focusing on what 'surveillance' itself means and therefore covering any device capable of conducting it.[130] As James Fleming, Executive Director of the Australian Institute of Employment Rights, a not-for-profit independent organisation that works to promote employment rights, stated, 'if you are too prescriptive, it is going to be quickly out of date.'[131] In other reports, the Australian Law Reform Commission and the Australian Human Rights Commission also argued for technology-neutral surveillance laws to avoid new technologies falling out of scope of regulation.[132]

Stakeholders also said that any state legislative changes should be amenable to national harmonisation in the future. This is especially important for businesses that operate across state and territory borders and for employers who have employees working remotely from interstate locations.[133] Kat Eather, General Counsel at the BCA, which represents over 130 of the nation's leading businesses, told the Committee that currently businesses that operate nationally will have a workplace surveillance policy that complies with the most stringent state legislation so that it would be lawful across all their operations.[134]

---

128 Dr Jake Goldenfein, *Transcript of evidence*, p. 52.

129 National Tertiary Education Union, *Submission 24*, p. 21; Danae Fleetwood, *Transcript of evidence*, p. 22; Amelia Bitsis, *Transcript of evidence*, p. 14; Dr Jacqueline Meredith, *Transcript of evidence*, p. 7.

130 Centre for Decent Work and Industry, *Submission 13*, p. 12; Danae Fleetwood, *Transcript of evidence*, p. 23.

131 James Fleming, Executive Director, Australian Institute of Employment Rights, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 4.

132 Australian Law Reform Commission, *Serious invasions of privacy in the digital era*, p. 282; Australian Human Rights Commission, *Protecting cognition: background paper on human rights and neurotechnology*, Sydney, 2024, p. 36.

133 Business Council of Australia, *Submission 5*, p. 1; Professor Peter Leonard, *Submission 8*, p. 2; Commonwealth Bank of Australia, *Submission 44*, p. 3; Amelia Bitsis, *Transcript of evidence*, p. 14; Chris Molnar, *Transcript of evidence*, pp. 23–24; Sunil Kemppi, Vice President, Employee Representative, Australian Institute of Employment Rights, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 3; Peter Johnson, *Transcript of evidence*, p. 10.

134 Kat Eather, *Transcript of evidence*, p. 19.

The need for harmonised regulation was also raised in the Australian House of Representatives Standing Committee on Employment, Education and Training's recent Inquiry into the digital transformation of workplaces tabled in February 2025 and discussed further in Chapter 1. The Standing Committee recommended the Australian Government work with the states and territories to develop better and more consistent protections against excessive or unreasonable workplace surveillance.[135]

Ideally, the Commonwealth would introduce legislation to replace existing state and territory surveillance laws and create consistency and certainty; however, this could take decades and sometimes states need to make the first move and have other jurisdictions follow.[136]

Laws should ensure surveillance is reasonable, necessary and proportionate

A solution commonly raised in the evidence to ensure workplace surveillance laws are technology neutral and achieve a fair balance between employers' genuine needs for conducting surveillance and protecting workers' privacy was using a principles-based approach. Specifically, workplace surveillance laws should be based on the core principles of reasonableness, necessity and proportionality.[137]

These principles were also recommended by the NSW Legislative Council Select Committee investigating workplace surveillance laws, which recommended that:

> workplace surveillance must be permitted only if it is reasonable, necessary and proportionate, fair, accurate, accountable and does not intrude more than is absolutely necessary on the privacy of workers.[138]

The NSW Committee also recommended that workplace surveillance only be carried out following an application to a Magistrate specifying how the surveillance will be conducted, its purpose and who benefits from the collected data. However, the

---

135 Parliament of Australia, House of Representatives Standing Committee on Employment, Education and Training, *The future of work: Inquiry into the digital transformation of workplaces*, February 2025, p. 58.

136 Associate Professor Normann Witzleb, Faculty of Law, Monash University, and Faculty of Law, The Chinese University of Hong Kong, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 41; Brown and Witzleb, 'Big brother at work', p. 29; Australian Human Rights Commission, *Protecting cognition*, p. 36; Australian Law Reform Commission, *Serious invasions of privacy in the digital era*, p. 282.

137 Professor Peter Leonard, *Submission 8, Attachment 1*, p. 7; National Tertiary Education Union, *Submission 24*, p. 24; Office of the Victorian Information Commissioner, *Submission 39A*, p. 2; James Fleming, *Transcript of evidence*, p. 4; Sean Morrison, *Transcript of evidence*, p. 11; Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 45; Kat Hardy, Lead Organiser, Australian Services Union, Victorian Private Sector Branch, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 38; Dr Jean Linis-Dinco, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, pp. 24–25; Paris Nicholls, Senior National Industrial Officer, Manufacturing Division, Construction, Forestry and Maritime Employees Union, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 54; Jenny Kruschel, National Secretary, Textile Clothing Footwear, Manufacturing Division, Construction, Forestry and Maritime Employees Union, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 54; Stephen Fodrocy, Industrial Officer, Australian Manufacturing Workers' Union, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, pp. 55–56.

138 Parliament of New South Wales, Legislative Council Select Committee on the Impact of Technological and Other Change on the Future of Work and Workers in New South Wales, *Impact of technological and other change on the future of work and workers in New South Wales: final report—workplace surveillance and automation*, p. 24.

Committee heard that this requirement could be deemed excessive and would likely be a burden on employers and the judicial system.[139]

The same principles of reasonableness, necessity and proportionality underpin Victoria's Privacy and Data Protection Act and, as Sean Morrison explained, OVIC determines if a breach of a person's privacy has occurred based on whether the activity in question was pursuing a legitimate objective and if the activity was 'reasonable, necessary and proportionate to achieving that objective.'[140]

The Committee also heard that there should be a positive obligation on employers to demonstrate that workplace surveillance is for a legitimate purpose and that the surveillance is reasonable, necessary and proportionate to achieve that purpose.[141] OVIC suggested this could be achieved by requiring employers to undertake a privacy impact assessment and a security risk assessment. This would help employers to understand and document the reason for the proposed workplace surveillance and the associated privacy risks, evaluate how intrusive the surveillance might be for workers and determine whether less intrusive means could be used instead to achieve the stated objective.[142]

As discussed in Chapter 2, employers have valid reasons for workplace surveillance including protecting workers' safety, protecting property and better understanding work processes.[143] However, as Alana Ginnivan, Professional Officer at the Victorian Branch of the Australian Nursing and Midwifery Federation, which represents nurses, midwives and personal care workers, stated, 'it is not to say that we do not support the surveillance. As we all agree, there is a place, but it is the balance.'[144] The NTEU stated that if employers had to determine a legitimate objective for workplace surveillance and ensure that it was reasonable, necessary and proportionate, it would eliminate many cases where surveillance may cause direct or indirect harm to workers.[145]

Whether surveillance is considered reasonable and proportionate would depend on the type and extent of impact it has on workers' legitimate expectations of privacy, community interests (such as the health and safety of other individuals) and employers' ability to run a safe and productive workplace, as well as whether less intrusive alternatives exist to achieve the stated objective.[146] Alternatives could include effective training, better communication from management, or using spot checks, investigating specific incidents or monitoring only high-risk individuals in place of the continuous surveillance of all employees.[147]

---

139 Professor Peter Leonard, *Submission 8, Attachment 1*, p. 7.

140 Sean Morrison, *Transcript of evidence*, p. 10.

141 Office of the Victorian Information Commissioner, *Submission 39*, pp. 11–12; Office of the Victorian Information Commissioner, *Submission 39A*, p. 8; Alana Ginnivan, *Transcript of evidence*, p. 41.

142 Office of the Victorian Information Commissioner, *Submission 39*, p. 11; Office of the Victorian Information Commissioner, *Submission 39A*, p. 7.

143 Scott Barklamb, *Transcript of evidence*, p. 35.

144 Alana Ginnivan, *Transcript of evidence*, p. 41. Also see, Associate Professor Alysia Blackham, *Transcript of evidence*, p. 40.

145 National Tertiary Education Union, *Submission 24*, p. 24.

146 Professor Peter Leonard, *Submission 8*, p. 3; Eurofound, *Employee monitoring and surveillance*, p. 18.

147 Brown and Witzleb, 'Big brother at work', p. 27.

RECOMMENDATION 1: That the Victorian Government introduce new principles-based workplace surveillance legislation that is technology neutral, defines a workplace as wherever work occurs, and places a positive obligation on employers to prove through a risk assessment that any surveillance they conduct is reasonable, necessary and proportionate to achieve a stated legitimate objective.

Transparency and consultation are essential

A recurrent theme in the evidence was the need to mandate transparency and consultation with workers before workplace surveillance is implemented. By letting workers know in advance that they will be surveilled, disclosing how and why the surveillance will take place, and giving them a chance to have some input into how the surveillance will be used can increase the sense of fairness among workers and lessen the chance of worker resistance.[148]

Stakeholders suggested that Victoria implement notification, disclosure and consultation requirements, similar to those in the ACT model.[149] Specifically, employers should be required to give workers 14 days' written notice of when surveillance devices will be used in the workplace and disclose the purpose of the surveillance, the surveillance methods that will be used, when and where it will occur, how the resulting data will be used and stored, whether the data may be used for performance management or disciplinary processes and employees' rights around the surveillance and its use. New employees should also be informed of any surveillance that is in place before starting employment.

Employers should also be required to develop a workplace surveillance policy that specifies the above information, which they must provide to all workers and then reissue whenever the policy is updated.[150] Furthermore, covert surveillance undermines trust between employers and employees and should be restricted to cases where an employee is suspected of criminal activity and should require approval by a court or Magistrate as is the case in NSW and the ACT.[151]

---

148 Dr Dale Tweedie, *Submission 34*, p. 3; Institute for Public Policy Research, *Watching me, watching you*, p. 17; Joanna Bronowicka, et al., *'Game that you can't win'?: workplace surveillance in Germany and Poland*, European University Viadrina, Frankfurt, 2020, pp. 10–11.

149 Australian Lawyers Alliance, *Submission 7*, p. 7; Centre for Decent Work and Industry, *Submission 13*, p. 7; Community and Public Sector Union, *Submission 20*, p. 12; Victorian Trades Hall Council, *Submission 28*, p. 35; Australian Manufacturing Workers' Union, *Submission 31*, p. 20; Law Institute of Victoria, *Submission 37*, p. 4; Dr Jacqueline Meredith, *Transcript of evidence*, p. 5; Dr Fiona Macdonald, *Transcript of evidence*, p. 21; Tash Wark, Secretary, Australian Services Union, Victorian and Tasmanian Authorities and Services Branch, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 44; Liam Hanlon, Industrial Officer, Independent Education Union, Victoria Tasmania Branch, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 32.

150 Australian Lawyers Alliance, *Submission 7*, p. 10; Construction, Forestry and Maritime Employees Union, *Submission 17*, p. 6; Simon Hammersley, Research and Policy Adviser, Australian Services Union, Victorian and Tasmanian Authorities and Services Branch, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 49.

151 Australian Lawyers Alliance, *Submission 7*, p. 7; National Tertiary Education Union, *Submission 24*, p. 22; Victorian Trades Hall Council, *Submission 28*, p. 44; Law Institute of Victoria, *Submission 37*, p. 5; Dr Jacqueline Meredith, *Transcript of evidence*, p. 5.

The ACT legislation also has consultation provisions where employers are required to consult with employees before introducing workplace surveillance. The Committee heard that Victoria should introduce a similar requirement for meaningful consultation where workers have a chance to be involved in the design and governance of workplace surveillance.[152] Doing so would enhance workers' acceptance of surveillance and their sense of control and reduce their feelings of distrust and powerlessness.[153]

In the industrial relations space, it is generally accepted that employees may not use consultation to veto change and the ultimate decision remains with the employer.[154] However, the Committee heard that the consultation must be genuine and meaningful where workers have the opportunity to challenge the proposed surveillance and suggest alternative options, and employers should take these views into account.[155] Also the consultation should be ongoing, similar to OHS requirements to consult with workers about health and safety matters that may affect them.[156]

As Joe Calafiore, the Chief Executive Officer of WorkSafe Victoria, stated, 'open and transparent consultation … is really central to a productive and trusting workplace.'[157] His colleague and WorkSafe's Principal Psychological Health and Safety Specialist, Amy Salmon, agreed saying:

> psychological harm is increased when workplace surveillance is used inappropriately, and that is including where it is not used transparently, where there is not consultation with employees about how it is being gathered and how it is being used or if there is a misalignment between that. Consultation is so key. That is really at the heart of whether it is going to create a risk or not create a risk.[158]

Adopting similar notification, disclosure and consultation practices to the ACT model would reduce the risk of harm caused by workplace surveillance.

RECOMMENDATION 2: That the Victorian Government include requirements for notification and disclosure in new workplace surveillance legislation that oblige employers to give 14 days' written notice to workers of workplace surveillance and that the notice specifies the methods, scope, timing and purpose of the surveillance and how the surveillance data will be used and stored.

---

152 Victorian Trades Hall Council, *Submission 28*, p. 35; Australian Manufacturing Workers' Union, *Submission 31*, pp. 14, 21; Dr Dale Tweedie, *Submission 34*, p. 8; Law Institute of Victoria, *Submission 37*, p. 5; Professor John Howe, *Transcript of evidence*, p. 3; Nicole McPherson, *Transcript of evidence*, p. 40; Tash Wark, *Transcript of evidence*, p. 44.

153 Australian Manufacturing Workers' Union, *Submission 31*, p. 21; Law Institute of Victoria, *Submission 37*, p. 5; Danae Fleetwood, *Transcript of evidence*, p. 21; Bronowicka, et al., *'Game that you can't win'?*, pp. 10–11.

154 Matt O'Connor, *Transcript of evidence*, p. 4.

155 Dr Dale Tweedie, Senior Lecturer, Department of Accounting and Corporate Governance, Macquarie University, public hearing, 26 September 2024, *Transcript of evidence*, p. 15; Stephen Fodrocy, *Transcript of evidence*, p. 56; Wilhemina Stracke, *Transcript of evidence*, p. 30.

156 Wilhemina Stracke, *Transcript of evidence*, p. 32; Dr Dale Tweedie, *Transcript of evidence*, p. 16.

157 Joe Calafiore, Chief Executive Officer, WorkSafe Victoria, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 23.

158 Amy Salmon, Principal Psychological Health and Safety Specialist, WorkSafe Victoria, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 23.

RECOMMENDATION 3: That the Victorian Government include the requirement in new workplace surveillance legislation for employers to consult with employees before introducing or changing surveillance practices in the workplace.

RECOMMENDATION 4: That the Victorian Government require employers who conduct surveillance to have a workplace surveillance policy that is provided to all employees and reissued to employees whenever the policy is updated.

RECOMMENDATION 5: That the Victorian Government restrict covert workplace surveillance to cases where an employee is suspected of unlawful activity, the employer has obtained a court order to undertake the surveillance, and an independent surveillance supervisor has been appointed to the case.

The use of AI with workplace surveillance needs extra protection

As discussed in Chapter 2, AI systems processing workplace surveillance data is a growing trend that employers are using for recruitment, task allocation, performance assessment, disciplinary action and termination. Many stakeholders were concerned about the risks of bias and discrimination when using AI in these ways, and in its proposal for enacting AI legislation, the European Union (EU) deemed the use of AI systems at work as high risk.[159]

In Europe, workers have the right to receive an explanation from employers about how an algorithm reached a decision and be able to request human intervention; however, in reality access to the algorithm or coding may be restricted by developers' proprietary interests and trade agreements.[160] The Committee heard that not only is transparency lacking around the underlying assumptions and algorithms used by AI systems in the workplace, there is also no guarantee that a person has actually reviewed decisions made by algorithms before significant employment outcomes such as discipline or termination occur.[161]

Furthermore, platform workers also have little transparency around how algorithms determine their job allocations, remuneration and removal from a platform.[162] In the EU, digital labour platforms must inform platform workers of the use of automated monitoring and decision-making systems, a human must oversee and evaluate the impact of these automated decisions at least every two years, and a human must

---

159 Blackham, 'Setting the framework for accountability for algorithmic discrimination at work', pp. 70–71.

160 Ibid., p. 83; Finance Sector Union, *Submission 35*, p. 12; Institute for Public Policy Research, *Watching me, watching you*, p. 24.

161 Community and Public Sector Union, *Submission 20*, p. 6; Kat Hardy, *Transcript of evidence*, p. 47.

162 Matt O'Connor, *Transcript of evidence*, p. 7; Sharon De Silva, Director, Secure Work, Industrial Relations Victoria, Department of Treasury and Finance, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 8.

make the final decision to restrict, suspend or terminate a platform worker's contract with the platform.[163]

The NSW Select Committee mentioned above that examined workplace surveillance recommended that OHS laws be amended to regulate the allocation of work by algorithms and platforms so workloads are safe and reasonable, promote fair and equitable distribution of work and are not discriminatory.[164]

In this current Inquiry, the Centre for Decent Work and Industry at the Queensland University of Technology, which is researching AI-enabled surveillance in the management of employees, called for greater transparency, formalised employee consultation and improved employer education about the risks, opportunities, ethics and obligations of using AI with workplace surveillance data.[165] Victorian unions also asked for transparency around how algorithmic decision-making determines outcomes in the workplace and a way for workers to be able to audit that decision-making.[166] The Co-Chair of the Law Institute of Victoria's Workplace Relations Committee, Chris Molnar, told the Committee that implementing notification and disclosure requirements around workplace surveillance would cover transparency around AI and algorithmic decision-making in employment decisions.[167]

Another solution would be to require human intervention when any automated decision significantly affects workers' lives. This would help to identify and correct mistakes or inaccuracies and ensure the employer is unable to use algorithmic decision-making to blur legal responsibility. Examples of such significant decisions would include promotion, reward, discipline or termination.[168] Alternatively, there could be a reverse onus on a human to prove that the AI systems or algorithmic decision-making used is reliable to make significant employment decisions.[169]

Enabling human intervention is one of ten guardrails in the Australian Government's Voluntary AI Safety Standard, which was developed to support and promote best practice in the safe and responsible use of AI systems. Although voluntary, this standard is designed to establish consistent practice across organisations and set

---

163 European Union, *Directive of the European Parliament and of the Council on improving working conditions in platform work*, Brussels, 2024, pp. 9–10; Blackham, 'Setting the framework for accountability for algorithmic discrimination at work', pp. 83–84, 88–89; Institute for Public Policy Research, *Watching me, watching you*, p. 14.

164 Parliament of New South Wales, Legislative Council Select Committee on the Impact of Technological and Other Change on the Future of Work and Workers in New South Wales, *Impact of technological and other change on the future of work and workers in New South Wales: final report—workplace surveillance and automation*, p. 44.

165 Centre for Decent Work and Industry, *Submission 13*, pp. 12–13.

166 Community and Public Sector Union, *Submission 20*, p. 6; Finance Sector Union, *Submission 35*, pp. 12–13; Laura Boehm, Industrial Officer, Australian Services Union, Victorian Private Sector Branch, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 48.

167 Chris Molnar, *Transcript of evidence*, p. 26.

168 Dr Fiona Macdonald and Dr Lisa Heap, Centre for Future Work, Australia Institute, *Inquiry into the digital transformation of workplaces*, submission to House of Representatives Standing Committee on Employment, Education and Training, 2024, p. 15; Blackham, 'Setting the framework for accountability for algorithmic discrimination at work', pp. 88–89; Ball, *Electronic monitoring and surveillance in the workplace*, p. 73; Future of Privacy Forum, *Best practices for AI and workplace assessment technologies*, Washington, 2023, p. 10.

169 Professor Peter Leonard, *Transcript of evidence*, p. 8.

expectations for what future legislation may look like.[170] In addition to enabling human control or intervention to achieve meaningful oversight of AI systems, some of the other guardrails that are relevant to workplace surveillance include informing end-users about AI-enabled decisions, and establishing processes for people to challenge the use or outcome of AI systems that have a personal impact on them.[171]

The principles guiding the Voluntary AI Safety Standard mirror the World Economic Forum's ethical principles when establishing a responsible AI program: fairness, transparency, accountability and privacy.[172] In addition, amendments to the Privacy Act in December 2024 will require Australian public service bodies and other entities covered by the Act to update their privacy policies if an AI system makes a decision that 'could reasonably be expected to significantly affect the individual's rights or interests.'[173] These entities would need to state the types of personal information that may be used by the AI system and the types of decisions that could be made. While it is a good step forward, this requirement will not take effect until December 2026 and even then, it is unclear whether it will go far enough to protect workers.[174]

In its Inquiry into the digital transformation of workplaces, the Australian House of Representatives Standing Committee on Employment, Education and Training recommended the Australian Government review the Fair Work Act and Privacy Act to require employers to notify and meaningfully consult with employees about 'the use of surveillance measures and data used by AI systems in the workplace.'[175] It also recommended that the Government work with Safe Work Australia, the nation's work health and safety regulator, to develop a Code of Practice that sets limits on how workplaces use AI and automated decision-making so as to reduce associated psychosocial risks.[176] The Australian Government had not responded to these recommendations by the time this current Inquiry report on Victorian workplace surveillance was adopted.

Dr Goldenfein pointed out that any standards or legislation around AI will not likely set out prescribed uses for AI but will instead specify compliance obligations such as transparency and oversight. He added that for this reason, Victoria should not rely on AI standards or legislation to protect workers from any harm arising from algorithmic decision-making using workplace surveillance data.[177] A specific requirement around

---

170 Department of Industry, Science and Resources, National Artificial Intelligence Centre, *Voluntary AI safety standard*, Australian Government, August 2024, p. iv.

171 Ibid.

172 Jim Stratton, 'The future of work starts with trust: how can we close the AI trust gap?', *World Economic Forum*, 15 January 2024, <https://www.weforum.org/stories/2024/01/why-there-is-an-ai-trust-gap-in-the-workplace> accessed 17 July 2024.

173 Sophie Dawson, Emily Lau and Lydia Cowan-Dillon, 'Practical implications of the new transparency requirements for automated decision making', *Johnson Winter Slattery*, 14 January 2025, <https://jws.com.au/what-we-think/practical-implications-of-new-transparency-requirements-for-automated-decision-making> accessed 20 January 2025.

174 Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 46.

175 Parliament of Australia, House of Representatives Standing Committee on Employment, Education and Training, *The future of work*, p. 58.

176 Ibid.

177 Dr Jake Goldenfein, *Transcript of evidence*, p. 52.

human intervention in algorithmic decision-making similar to that operating in the EU would overcome this.

RECOMMENDATION 6: That the Victorian Government require employers have a person with delegated authority review any automated decision made using workplace surveillance data that could significantly affect the rights, interests or employment status of a worker, including a platform worker.

Requirements to disclose and consult should have minimal impact on businesses

As discussed earlier in the chapter, business groups made it clear that whatever changes to workplace surveillance regulation the Committee decides to recommend, they should not impose further burdens on employers or create inconsistencies for businesses that operate across multiple states.[178] Requiring Victorian employers to meet the same notice and disclosure obligations as employers in NSW and the ACT, as well as match the ACT's employee consultation requirements, should not be too onerous on businesses, especially those already operating nationally that have a business-wide policy that complies with laws in the most stringent jurisdictions.[179]

Kat Eather from BCA and Yoness Blackmore, Ai Group's Principal Advisor on Workplace Relations Policy, both noted that most employers understand it is in their interests to be transparent about workplace surveillance because it reduces any potential psychological harm to workers and can minimise the risks of any unfair dismissal or compensation claims in the future.[180] As Kat Eather stated:

> the BCA would accept that it is reasonable for employers to give notice to their employees about surveillance taking place … I think most employers would accept that that is a reasonable approach.[181]

Similarly, under OHS laws, Victorian employers already have a duty to consult with their employees on an ongoing basis about health and safety matters that affect them, so having a similar requirement for workplace surveillance should not be too much of an additional burden.[182] As Chris Molnar from the Law Institute of Victoria stated:

> there are quite significant obligations to consult in the OHS legislation … employers that are aware do engage in those sorts of processes. I do not see that as a big cost. I see that as simply a process, and it is consistent with a lot of the other obligations which employers have these days.[183]

---

178 Kat Eather, *Transcript of evidence*, p. 22; Georgia Holmes, Policy and Communications Advisor, Master Electricians Australia, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 26; Name withheld, *Submission 30*, p. 1.

179 Matt O'Connor, *Transcript of evidence*, p. 10.

180 Kat Eather, *Transcript of evidence*, pp. 20–21; Yoness Blackmore, *Transcript of evidence*, p. 33.

181 Kat Eather, *Transcript of evidence*, p. 20.

182 Daniel Hodges, Executive Manager, Workplace Relations, Victorian Automotive Chamber of Commerce, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 32.

183 Chris Molnar, *Transcript of evidence*, p. 25.

Matt O'Connor, Deputy Secretary of Industrial Relations Victoria, which is the Victorian Government's lead agency for developing industrial relations policy and initiatives, agreed stating:

> if you look at New South Wales and the ACT, the obligation is to notify and to consult. You might need additional resources perhaps in terms of a HR resource to manage something like that. So I do not see that being in itself a huge cost. I think the cost is in buying the stuff [surveillance technology] in the first place, probably.[184]

Regarding any additional requirements on employers, previous reviews by the Australian and Victorian law reform commissions did not accept that removing the employee records exemption from the Privacy Act and introducing workplace surveillance laws, respectively, would create a significant burden on employers.[185] In fact, businesses that do not conduct intrusive workplace surveillance would have relatively few costs.[186]

FINDING 20: Requiring employers to disclose details and consult with workers about introducing or changing surveillance practices in the workplace would not impose a significant burden on employers and would reduce the risk of harm to workers and potential unfair dismissal or compensation claims in the future.

Business groups were also concerned that small businesses would struggle the most with any changes in workplace surveillance regulation because they lacked the OHS, legal and human resources that larger businesses have. They suggested the Victorian Government should focus on providing information and encouragement instead by developing best-practice workplace surveillance guidelines.[187] However, Dr Blackham from the NTEU suggested that small businesses would probably be the least affected because they would be less likely to use sophisticated workplace surveillance devices than large businesses. She told the Committee:

> I would anticipate though that small businesses often are run more informally and they are less reliant on these sorts of technological surveillance mechanisms because you are seeing everyone in the workplace every day and you can manage people in that interpersonal way, which often gets lost in a large organisation. So I would say perhaps small business will be less affected by changes in this area and this is more likely to impact larger employers where they are managing large workforces and trying to do that at scale using technology and relying on quantitative metrics rather than that interpersonal relationship.[188]

---

184 Matt O'Connor, *Transcript of evidence*, p. 9.

185 Heap, *No blood—no job*, p. 27; Brown and Witzleb, 'Big brother at work', p. 24.

186 Brown and Witzleb, 'Big brother at work', p. 24.

187 Scott Barklamb, *Transcript of evidence*, p. 36; Yoness Blackmore, *Transcript of evidence*, pp. 34, 37; Daniel Hodges, *Transcript of evidence*, pp. 31, 32; Amelia Bitsis, *Transcript of evidence*, p. 21.

188 Associate Professor Alysia Blackham, *Transcript of evidence*, p. 45.

Dr Meredith from Swinburne University was concerned that there is no guarantee that employers will follow best-practice guidelines if they are not enforceable.[189] Her colleague Professor Holland stressed the importance of safeguards around workplace surveillance saying:

> We are not looking at draconian measures; we are saying it is important that managers understand that there is a lot of information being gathered here. You need to understand why you are doing it, if you need to do it and how you are managing that information.[190]

The Victorian Government and WorkSafe Victoria assured the Committee that if workplace surveillance reforms were introduced, they would provide education materials and support services and work with employer groups to develop and disseminate education, advice and assistance to individual employers. The material would include online resources, face-to-face consultation and hard copy resources, webinars and roadshows.[191]

RECOMMENDATION 7: That the Victorian Government work with employer groups to provide education and support services and material to employers about any changes to workplace surveillance regulation.

4.2.3 Workers also need protection against surveillance by third parties

A supplementary issue raised in the evidence was the unauthorised surveillance of employees in the workplace by third parties, that is, individuals who are not their employer. Examples included nurses, midwives and aged care workers filmed by families and patients in healthcare facilities or in the home when providing domiciliary midwifery or Hospital in the Home care.[192] Without regulation of such filming via phones and other devices, health and aged care workers are placed in a difficult position if they want to challenge this surveillance, and this can result in psychological stress.[193]

Workers in schools also lack protection from surveillance by students or parents while in the workplace. The Victoria Tasmania Branch of the Independent Education Union (IEU), which represents staff in non-government education settings, said students are either overtly or covertly filming teachers in the classroom or schoolyard without their

---

189 Dr Jacqueline Meredith, *Transcript of evidence*, p. 6.

190 Professor Peter Holland, Professor, Human Resource Management, School of Business, Law and Entrepreneurship, Swinburne University of Technology, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 6.

191 Matt O'Connor, *Transcript of evidence*, pp. 9, 10–11; Joe Calafiore, *Transcript of evidence*, p. 25; Amy Salmon, *Transcript of evidence*, p. 28.

192 Ramsay Health Care Australia, *Submission 15*, pp. 2–3; United Workers Union, *Submission 25*, p. 9; Australian Nursing and Midwifery Federation, *Submission 38*, p. 8.

193 United Workers Union, *Submission 25*, p. 9; Libby Muir, Professional Officer, Australian Nursing and Midwifery Federation, Victorian Branch, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, pp. 39–40.

consent and then uploading the footage to social media.[194] For example, David Brear, General Secretary of the IEU's Victoria Tasmania Branch, told the Committee:

> every student has an iPhone, every student has got an iPad or a laptop computer with a camera in it. A lot of students have got smartwatches, so we have had instances of students ringing their parent during class and then a teacher being transmitted through the smartwatch into a conversation with a parent and not knowing that that was going on … We get instances, for example, of students deliberately provoking a teacher; someone will be filming it and then someone will deliberately provoke someone and then get a particular response that will then be uploaded onto TikTok or something like that.[195]

Students could use such actions to bully, intimidate or harass a worker and uploading footage to social media can cause reputational damage for teachers.[196]

The Victorian Department of Education has a policy about recording staff and other adults in government schools, which as a general rule requires consent, but the policy does not specifically mention recording by students or parents.[197] School workers in such situations have no protection under the Victorian Surveillance Devices Act because the activities and conversations are recorded in circumstances where they would not be considered private. And even though the Privacy Act applies to employers in the non-government education sector, it does not cover breaches by students. Ultimately, any sanction is at the discretion of the school, which may experience pressure from fee-paying parents not to discipline their child.[198]

While teachers do not necessarily want students to be prosecuted under legislation, they do want to be able to do their job without having to worry about being recorded and they do not want surveillance by students to intimidate other students from participating in class for fear of being filmed.[199] The IEU suggested that the Surveillance Devices Act be amended to require employers to take all reasonable steps to ensure individuals do not engage in surveillance of workers without workers' consent.[200] Alternatively, the Victorian Registration and Qualifications Authority, which registers non-government schools, could mandate that schools must have a policy around students recording teachers and other school staff in the workplace.[201]

---

194 Independent Education Union, Victoria Tasmania Branch, *Submission 23*, p. 2; Liam Hanlon, *Transcript of evidence*, p. 29.

195 David Brear, General Secretary, Independent Education Union, Victoria Tasmania Branch, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 30.

196 Independent Education Union, *Submission 23*, p. 3.

197 Department of Education, Victoria, *Photographing, filming and recording staff and other adults*, 2020, <https://www2.education.vic.gov.au/pal/photographing-staff/policy> accessed 6 February 2025.

198 Independent Education Union, *Submission 23*, pp. 2–3.

199 David Brear, *Transcript of evidence*, p. 32; Liam Hanlon, *Transcript of evidence*, p. 34.

200 Independent Education Union, *Submission 23*, p. 4.

201 David Brear, *Transcript of evidence*, p. 30.

This is another instance where Victorian surveillance legislation has not kept pace with technological advances and the widespread use of devices with recording functions, such as laptops and mobile phones, among all members of society. Employees' privacy while at work should be protected from unauthorised surveillance by third parties.

FINDING 21: Employees' privacy is at risk from unauthorised surveillance by third parties in the workplace, which can cause psychological stress and possibly reputational damage if recordings are disseminated through social media or other media channels.

RECOMMENDATION 8: That the Victorian Government require employers to take all reasonable steps to prevent surveillance of an employee while at work by a party other than the employer without the employee's consent.

The Victorian Farmers Federation (VFF), which is a lobby group that promotes the interests of farmers, had similar concerns about animal activists trespassing onto farms and installing surveillance devices to record on-farm practices that are then packaged and distributed to media outlets. While such surveillance is unlawful under the Surveillance Devices Act, it is exempted under a public interest clause.[202]

The VFF claimed this surveillance breached the privacy of farmers and their families and could cause reputational damage if footage is published out of context and lead to stress and anxiety for farmers, their families and staff. It called for the public interest exemption to be narrowed or for it to be removed to match the legislation in NSW as well as making surveillance undertaken through an act of trespass unlawful.[203] The Committee recognises that unauthorised surveillance of farms causes stress and anxiety for farmers; however, this type of surveillance falls outside of the Inquiry's scope, which focuses on the surveillance of employees in the course of their employment, rather than the recording of business practices.

---

202 Victorian Farmers Federation, *Submission 16*, p. 3; Emma Germano, President, Victorian Farmers Federation, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 30.

203 Victorian Farmers Federation, *Submission 16*, p. 4; Emma Germano, *Transcript of evidence*, p. 30; Charles Everist, General Manager, Policy and Advocacy, Victorian Farmers Federation, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 32.

Chapter 5
Surveillance data and employee privacy

There are two types of privacy: physical privacy and information privacy. Physical privacy is concerned with access to individuals' bodies and their physical surroundings and information privacy with access to individuals' personal information. In terms of workplace surveillance, information privacy can be seen as employees' ability to control who can see or use their personal information, how and when this information is collected and how it can be used.[1]

According to the Fair Work Ombudsman, personal information is 'information that says who we are, what we do and what we believe.'[2] It includes names, contact details, photos, bank account details, tax file numbers, driver licence details and work records such as performance evaluations. A subset of this is sensitive personal information, which includes information about a person's health, ethnicity, sexual orientation, political associations, religious beliefs, trade union memberships, criminal records and biometric data. Sensitive personal information generally attracts a higher level of privacy protection.

This chapter is concerned with the impact workplace surveillance has on employees' information privacy. It starts by considering Victorian employers' current practices around handling workplace surveillance data, before examining the effectiveness of current Victorian and federal data privacy laws and then concluding with ways to strengthen privacy protections around workplace surveillance data.

5.1 Employers' data handling is not transparent risking workers' privacy

The Committee heard that the unprecedented volumes of data currently collected in the workplace about employees is concerning when most employees do not know how this data is stored, used or disclosed, how long it is kept, when and how it is disposed of, who has access to it and whether it can be sold on.[3]

---

1 Mena Angela Teebken and Thomas Hess, 'Privacy in a digitised workplace: towards an understanding of employee privacy concerns', *Proceedings of the 54th Hawaii International Conference on System Sciences*, 2021, p. 6662.

2 Fair Work Ombudsman, *Workplace privacy best practice guide*, Australian Government, 2023, p. 2.

3 Centre for Decent Work and Industry, QUT, *Submission 13*, p. 6; Professor Peter Holland and Dr Jacqueline Meredith, Swinburne University of Technology, *Submission 22*, p. 9; Victorian Trades Hall Council, *Submission 28*, p. 15; Australian Manufacturing Workers' Union, *Submission 31*, p. 16; Finance Sector Union, *Submission 35*, p. 4; Professor John Howe, Centre for Employment and Labour Relations Law, Melbourne Law School, University of Melbourne, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 1; Chris Lehmann, General Manager, Membership, Advocacy and Partners, Master Electricians Australia, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 29; Nicole McPherson, National Assistant Secretary, Finance Sector Union, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 40; Associate Professor Alysia Blackham, National Tertiary Education Union, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 46; Teebken and Hess, 'Privacy in a digitised workplace', p. 6669.

The Office of the Victorian Information Commissioner (OVIC), which regulates the collection, use and disclosure of personal information in the Victorian public sector (VPS), mentioned that VPS staff are concerned about their employers' surveillance practices based on enquiries it has had about data security controls and retention policies, employers' access to employee devices used for professional and personal use, surveillance policy requirements and the circumstances in which surveillance data can be used, accessed or disclosed.[4] As the Victorian Information Commissioner Sean Morrison explained, 'we have not got a flood of complaints, but it is going to be the next frontier.'[5]

This section considers employers' collection, sharing, sale, disclosure and disposal practices around workplace surveillance data, and then looks at the associated privacy and data security risks these practices pose.

5.1.1 Workers are left in the dark about how their data is used, shared and stored

The Committee did not receive a large amount of evidence regarding how Victorian employers are handling workplace surveillance data, which corroborates stakeholders' comments around the lack of transparency surrounding how workplace surveillance data is collected, used, shared and stored.

According to the Australian HR Institute, the professional body that supports human resources in Australia, '[p]roper management of surveillance data, including its collection, sharing, storage, disclosure, and disposal, is vital for protecting employee privacy.'[6] It polled 74 of its members and found that 19% of organisations use third-party services to manage surveillance data and the other 81% follow internal procedures, which highlights the need for agreed minimum standards on the secure and ethical handling of workplace surveillance data.[7]

As mentioned throughout this report, and covered more thoroughly in Section 5.2, current state and federal data privacy laws only apply to the public sector (and federally, to entities with an annual turnover above $3 million), so most employers are not bound by any privacy regulation relating to their employees' data.

The Commonwealth Bank of Australia explained how federal privacy laws require it to be open and transparent with its employees about how their personal information is managed, and that its privacy policy and information security framework govern the use and disclosure of personal information to protect against unlawful or unauthorised processing and accidental or unlawful disclosure, access, destruction, loss or modification.[8]

---

4 Office of the Victorian Information Commissioner, *Submission 39*, p. 7.

5 Sean Morrison, Victorian Information Comissioner, Office of the Victorian Information Commissioner, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 13.

6 Australian HR Institute, *Submission 10*, p. 2.

7 Ibid., pp. 2–3.

8 Commonwealth Bank of Australia, *Submission 44*, p. 3.

However, without similar obligations imposed on small businesses, there is a lack of guardrails to protect all employees' workplace surveillance data and privacy. Sean Morrison told the Committee that he is concerned about the security controls around workplace surveillance data. He said despite the best intentions of employers, there are no controls around data access, disclosure and use, and no audit program or risk framework to assess and manage privacy risks.[9]

As discussed in Chapter 2, employers are collecting vast amounts of information on employees through optical, listening, data and tracking surveillance devices in the workplace. The COVID-19 pandemic and the shift to remote working intensified workplace surveillance and the collection of employee data, which extended to information about vaccination status, health-related information and travel history.[10]

Professor Peter Holland from the Human Resource Management Department at Swinburne University of Technology's School of Business, Law and Entrepreneurship, believes both managers and employees do not completely understand the significance and implications of collecting such data, and the lack of transparency around the purpose of collecting it and its use is problematic because workers are unable to make informed decisions about the collection of this information.[11] Alana Ginnivan, Professional Officer at the Victorian Branch of the Australian Nursing and Midwifery Federation (ANMF), which represents nurses, midwives and personal care workers, added that its members are required to show they have a certain level of immunity to vaccine-preventable diseases to be permitted to work, but it is unclear to employees how this data is stored and distributed.[12]

The lack of transparency around how workplace surveillance data is stored was echoed by other stakeholders. For example, Paris Nicholls, Senior National Industrial Officer at the Manufacturing Division of the Construction, Forestry and Maritime Employees Union (CFMEU), told the Committee:

> it raises lots of issues that our members and I do not even entirely understand to do with how the data is stored digitally, how it is protected and what sorts of assurances our members and workers can have that it is actually being protected. Obviously there have been some pretty high-profile data breaches in the country and around the world, so trying to get that level of transparency is something that is really difficult.[13]

Larger employers tend to be more transparent about their processes due to their obligations under the Privacy Act. For example, Ramsay Health Care Australia explained how all its closed-circuit television (CCTV) footage is stored on a local server

---

9 Sean Morrison, *Transcript of evidence*, p. 11.

10 Attorney-General's Department, *Privacy Act review: report*, Australian Government, Canberra, 2022, p. 65.

11 Professor Peter Holland, Professor, Human Resource Management, School of Business, Law and Entrepreneurship, Swinburne University of Technology, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, pp. 1–2.

12 Alana Ginnivan, Professional Officer, Australian Nursing and Midwifery Federation, Victorian Branch, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 44.

13 Paris Nicholls, Senior National Industrial Officer, Manufacturing Division, Construction, Forestry and Maritime Employees Union, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 53.

and recorded over every 7, 14 or 28 days and is only disclosed to law enforcement and only upon receipt of a subpoena.[14]

However, the Committee also heard that some employers outsource the collection, management and storage of workplace surveillance data to one or more external companies, and often workers are not informed of where their data is going and what safeguards these third-party companies have in place to secure the data and not share it with other parties.[15]

The Committee also heard that there have been cases overseas where employers or third-party software providers have on-sold workplace surveillance data to data brokerage firms or private companies without workers' consent.[16] One such data brokerage firm based in the United States of America, Argyle, has access to workers' payroll, taxation, superannuation, pre-employment check and reporting data from companies such as Amazon, Walmart, Starbucks, Uber, FedEx, and Target, which it sells to its clients, who are mostly payday loan providers but also general loan servicers, lenders and insurers. These workers would not know that their information has been sold to third parties and it potentially places financially vulnerable workers at risk of predatory behaviours from high-interest payday loan providers.[17]

It is also unclear who owns workplace surveillance data; if the employer collects the data, then it is likely that it also owns the data, but if the data is collected by another firm that is running the surveillance software then it would depend on the contract between the employer and software provider.[18] When it comes to private investigators collecting data for a workplace investigation, the data is supplied back to the employer that commissioned the investigation and who now owns it. However, investigators would also retain the data for at least seven years for potential litigation or insurance purposes.[19]

FINDING 22: There is little transparency around how Victorian employers are currently using, sharing and storing workplace surveillance data.

---

14 Ramsay Health Care Australia, *Submission 15*, p. 2.

15 Australian Manufacturing Workers' Union, *Submission 31*, p. 16; Michael Johns, CEO, Bundle Australia, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 14; Associate Professor Alysia Blackham, *Transcript of evidence*, p. 44; Alysia Blackham, 'Surveillance, data collection and privacy at work: a new application of equitable obligations?', *Australian Journal of Labour Law*, (forthcoming), 2025, p. 20.

16 The Centre for Future Work, Australia Institute, *Submission 32*, p. 2; Adjunct Professor Moira Paterson, Castan Centre for Human Rights Law, Faculty of Law, Monash University, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, pp. 45–46; Professor John Howe, *Transcript of evidence*, p. 2.

17 Colleen Chen and John Howe, *Worker data right: the digital right of entry*, policy brief, no. 5, Centre for Employment and Labour Relations Law, University of Melbourne, 2022, pp. 5, 6.

18 Professor John Howe, *Transcript of evidence*, p. 2; Australian Nursing and Midwifery Federation, Victorian Branch, *Submission 38*, p. 6.

19 Jody Wright, CEO, Institute of Mercantile Agents, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 18.

5.1.2 Privacy and data security threats escalate as workplace surveillance grows

As workplace surveillance proliferates and employers collect and retain greater amounts of data about their employees, the risk of employees' privacy being breached escalates. Since most of this data is stored digitally, workers' personal information is particularly vulnerable to data breaches, exposing workers to privacy risks such as identity fraud and reputational damage.[20] Data breaches can occur when data held by an organisation is accessed, modified or disclosed without authorisation, misused or lost. This can be deliberate by either an internal or external party or inadvertent through human error or poor data management.[21]

Individuals' right to privacy is recognised as a fundamental human right in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the Victorian Charter of Human Rights and Responsibilities.[22] As OVIC explained:

> Privacy is central to an individual's right to live a full, free and dignified life, without fear of coercion or persecution for who they are or what they choose to believe. In this way, privacy is closely interlinked with other human rights such as the freedom of conscience, thought and belief, freedom of expression and freedom of association.[23]

However, privacy is a non-absolute right, which means that there are limitations if interference with a person's privacy is seen as legitimate, reasonable, necessary and proportionate. For example, a bank monitoring workers' transactions to prevent and detect fraud. Therefore, workplace surveillance that meets these requirements would not contravene the right to privacy.[24]

The Committee heard of situations where the collection of workplace surveillance data is not meeting these requirements and is threatening the privacy of employees and their families. For example, work laptops used remotely that can pick up private conversations held in the background; dash cameras in vehicles recording conversations and activities outside of work hours; devices for work and personal use giving employers access to personal information such as banking details, passwords, medical records and correspondence; facial recognition technology used with CCTV surveillance to track individuals' activities; and body-worn cameras in healthcare settings capturing others' health and personal information.[25]

---

20 The Centre for Future Work, *Submission 32*, p. 3; Office of the Victorian Information Commissioner, *Submission 39*, p. 8; Attorney-General's Department, *Privacy Act review*, p. 1.

21 Office of the Victorian Information Commissioner, *Submission 39*, p. 8.

22 Ibid., p. 2; Australian Law Reform Commission, *Serious invasions of privacy in the digital era: final report*, Australian Government, Sydney, 2014, pp. 30, 35.

23 Office of the Victorian Information Commissioner, *Submission 39*, p. 2.

24 Ibid., pp. 10–11; Information Commissioner's Office UK, *Employment practices and data protection: monitoring workers*, October 2023, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers> accessed 14 May 2024.

25 Institute of Mercantile Agents, *Submission 14*, p. 4; Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 8; Australian Nursing and Midwifery Federation, *Submission 38*, p. 8; Australian Education Union, Victorian Branch, *Submission 42*, p. 3; Professor Peter Holland, *Transcript of evidence*, p. 2.

In another instance, a company in Craigieburn, Victoria, that prints polymer banknotes has recently introduced a requirement for its employees to provide the following personal information to an interstate third party to 'assist its commercial negotiations with customers': full birth certificate; all passports held within the previous 10 years; current photograph; character references; names, nationalities and birthdates of family members; club, association or interest group memberships; and criminal history. Some members of the Australian Manufacturing Workers' Union (AMWU), which represents workers in all areas of manufacturing, are uncomfortable with providing this information and are worried about its security, but not supplying this information could lead to dismissal.[26]

Conversely, employees can also be concerned about the security of work data on their personal devices. For example, remote workers who are required to install work programs or save work data on their own devices may be worried about risks to the security of this data if the device is also used by family members or if they are subject to a data breach.[27]

The risk posed by hacking was raised multiple times in the evidence, especially when employers retain surveillance data for longer periods than needed.[28] The impact of hacking or a data breach depends on the type of information that is held, so workplace surveillance activities that are more intrusive will have a greater potential for negative consequences if the data is accessed maliciously, as will collecting data beyond what is necessary for work functions and storing this data for extended periods of time, even after employees have left the organisation.[29]

This is even more important for biometric data such as facial recognition, iris scans or fingerprints, because if compromised this data cannot be reissued or cancelled (unlike a password for example). The consequences could be severe for a worker whose biometric data has been compromised such as ongoing identity fraud.[30]

While federal privacy laws cover customer data, there are no such protections for workers' data if companies are hacked.[31] The Building Industry Group of Unions, which is comprised of the Electrical Trades Union, Plumbing and Pipe Trades Employees Union, AMWU and the CFMEU, added that it was unacceptable for workers to not know how their data is being stored and by whom (for example, a third party) when data breaches in organisations are so common now.[32]

---

26 Australian Manufacturing Workers' Union, *Submission 31*, pp. 12–13; Building Industry Group of Unions, *Submission 36*, p. 5.

27 Teebken and Hess, 'Privacy in a digitised workplace', p. 8.

28 Centre for Decent Work and Industry, *Submission 13*, p. 9; Institute of Mercantile Agents, *Submission 14*, pp. 3–4; Construction, Forestry and Maritime Employees Union, Manufacturing Division, *Submission 17*, p. 3; Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 8; Office of the Victorian Information Commissioner, *Submission 39*, p. 5; Professor Peter Holland, *Transcript of evidence*, pp. 2, 8; Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 45; Alana Ginnivan, *Transcript of evidence*, p. 47; Attorney-General's Department, *Privacy Act review*, p. 68.

29 Office of the Victorian Information Commissioner, *Submission 39*, p. 9.

30 Ibid., pp. 6–7; Professor Peter Holland, *Transcript of evidence*, p. 7; Peter Holland and Tse Leng Tham, 'Workplace biometrics: protecting employee privacy one fingerprint at a time', *Economic and Industrial Democracy*, vol. 43, no. 2, 2022, p. 504.

31 Centre for Decent Work and Industry, *Submission 13*, p. 9; Associate Professor Alysia Blackham, *Transcript of evidence*, p. 46; Attorney-General's Department, *Privacy Act review*, p. 68.

32 Building Industry Group of Unions, *Submission 36*, p. 7.

FINDING 23: Employers who retain workplace surveillance data unnecessarily or do not securely store it increase the risk that employees' personal information may be misused or accessed inappropriately or maliciously.

5.2 Current privacy laws are ineffective at protecting workers' data

As with workplace surveillance regulation discussed in Chapter 4, privacy laws at both the federal and state/territory levels do not fully protect the privacy of employees' data collected through workplace surveillance.[33] According to Professor Peter Leonard, a lawyer and data and technology business consultant, there are no baseline human rights statutes in Australia that laws addressing data privacy have to be considered against, and often these laws do not actually define data privacy or how their rules about data handling address privacy.[34]

More specifically, current privacy laws incorporate a number of exemptions that result in a large proportion of employees having minimal privacy protection in terms of their workplace surveillance data.[35] This section discusses the effectiveness of privacy laws for protecting employee privacy in Victoria, interstate and federally before considering overseas regulation of data protection, Australia's obligations under international conventions and best practice examples.

5.2.1 Victoria's privacy laws are limited to the public sector

Along with Queensland and the Australian Capital Territory (ACT), Victoria is one of three Australian jurisdictions with a human rights charter. The *Charter of Human Rights and Responsibilities Act 2006* (Vic) protects individuals' right to not have their privacy arbitrarily interfered with. However, it has some limitations: the Act only applies to public entities, individuals cannot make complaints directly to a court or tribunal for breaches of the Charter alone, and remedies for breach of the Charter do not include damages. These limitations have resulted in few claims made against the Charter.[36]

---

33 Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 9; Lisa Heap, *No blood—no job: Australia's privacy laws and workers' rights*, Centre for Future Work, Australia Institute, 2024, p. 9; Parliament of New South Wales, Legislative Council Select Committee on the Impact of Technological and Other Change on the Future of Work and Workers in New South Wales, *Impact of technological and other change on the future of work and workers in New South Wales: final report—workplace surveillance and automation*, November 2022, pp. 20–21.

34 Peter Leonard, 'Workplace surveillance and privacy', *Computers and Law: Journal for the Australian and New Zealand Societies for Computers and the Law*, vol. 93, 2021, pp. 63, 67.

35 Office of the Victorian Information Commissioner, *Submission 39*, p. 3.

36 Blackham, 'Surveillance, data collection and privacy at work', p. 8; Victorian Equal Opportunity and Human Rights Commission, *Charter complaints and remedies*, <https://www.humanrights.vic.gov.au/for-public-sector/charter-complaints-and-remedies> accessed 30 January 2025.

As discussed in Chapter 1, the primary legislation in Victoria relating to data privacy is the *Privacy and Data Protection Act 2014* (Vic). It protects the privacy of personal information collected and held by VPS organisations, including that of their employees. It does not apply to the private sector unless a private organisation is a contracted service provider to the VPS, and then only in relation to the services provided under the contract and if the contract specifies a requirement for compliance with the Act's 10 Information Privacy Principles (IPPs) that govern how VPS organisations must handle personal information.[37] The IPPs are:

- IPP 1—Collection
- IPP 2—Use and disclosure
- IPP 3—Data quality
- IPP 4—Data security
- IPP 5—Openness
- IPP 6—Access and correction
- IPP 7—Unique identifiers
- IPP 8—Anonymity
- IPP 9—Transborder data flows
- IPP 10—Sensitive information.

Some of these IPPs directly relate to workplace surveillance. For example, IPP 1 requires VPS organisations to limit collection of personal information to what is necessary for business functions or activities. Organisations must also inform their employees of the purpose of data collection, to whom the data is disclosed and that an employee can request access to their data.[38]

IPP 2 limits the use and disclosure of personal information to the purpose for which it was collected, unless the VPS organisation is required to disclose it to a law enforcement agency investigating unlawful activity. IPP 4 requires VPS organisations to protect personal information from misuse, loss and unauthorised access, modification or disclosure by securely storing the data, and destroying or permanently de-identifying it when no longer needed. IPP 5 ensures that VPS organisations must be transparent about their data handling processes and have a clear and accessible privacy policy.[39]

---

37 National Tertiary Education Union, *Submission 24*, p. 15; Office of the Victorian Information Commissioner, *Submission 39*, p. 2; Office of the Victorian Information Commissioner, *Privacy during employment*, 2019, <https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-during-employment> accessed 10 May 2024; Blackham, 'Surveillance, data collection and privacy at work', p. 8.

38 Office of the Victorian Information Commissioner, *Submission 39*, p. 4.

39 Ibid., pp. 4–5.

IPP 9 restricts the transfer of personal information across state borders (which may occur if surveillance software stores data in servers outside of Victoria) to situations where the employee consents, the recipient is subject to a law with similar protections to the IPPs, or if the recipient is contracted to handle the data in a way consistent with the IPPs. Last, IPP 10 specifies the circumstances in which VPS organisations can collect sensitive personal information, such as when the employee has consented or it is required by law.[40]

Despite these protections, stakeholders raised some gaps in the Privacy and Data Protection Act that suggest it is not entirely effective at protecting the privacy of employees' data. For example, the Act's restriction to VPS organisations means there are no obligations on private sector organisations regarding the collection, disclosure, storage, sale and disposal of surveillance data, leaving the data of private sector employees unprotected.[41] The ANMF also raised the confusing overlap of legislation that applies in healthcare settings, with health information covered by the *Health Records Act 2001* (Vic), which is administered by the Health Complaints Commissioner.[42] It added that an individual complainant is unable to initiate proceedings in a court against a VPS employer for a privacy breach.[43] Furthermore, OVIC noted that the Act does not include biometric data as a type of sensitive personal information leaving this information unprotected by Victorian legislation.[44] This is covered in more detail in Section 5.3.2.

Results from a survey of its members by the National Tertiary Education Union (NTEU), which represents all higher education and university employees in Australia, suggest that there is poor compliance with the Privacy and Data Protection Act among Victoria's universities, which are bound by the Act. For example, members reported that they were unaware of the purposes their employers were using surveillance data for, that they could access the information collected by their employer and if their employer had a workplace surveillance policy.[45]

FINDING 24: The *Privacy and Data Protection Act 2014* (Vic) has several gaps, which means it is ineffective at protecting all employees' personal information; for example, it only applies to Victorian public sector organisations, and it does not recognise biometric data as a form of sensitive personal information.

40 Ibid., pp. 5–6.

41 National Tertiary Education Union, *Submission 24*, p. 15; Australian Workers' Union, *Submission 27*, p. 1; Office of the Victorian Information Commissioner, *Submission 39*, pp. 2–3; Victorian Government, *Submission 43*, p. 8; Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 44.

42 Australian Nursing and Midwifery Federation, *Submission 38*, p. 7.

43 Ibid.

44 Office of the Victorian Information Commissioner, *Submission 39*, p. 6.

45 National Tertiary Education Union, *Submission 24*, p. 16.

5.2.2 ACT is the only Australian jurisdiction to protect workplace surveillance data

The only Australian jurisdiction that regulates the handling of workplace surveillance data is the ACT. The *Workplace Privacy Act 2011* (ACT) requires an employer to 'take reasonable steps to protect surveillance records it holds from misuse, loss, unauthorised access, modification or disclosure' as well as to destroy or permanently de-identify records it no longer needs.[46] In addition, the *Information Privacy Act 2014* (ACT) contains 13 Territory Privacy Principles that govern how public sector authorities in the ACT handle personal information, and the right to privacy is protected by a human rights charter that requires public authorities to act in a way that is compatible with the rights.[47]

New South Wales, which along with the ACT is the only other Australian jurisdiction to have dedicated workplace surveillance laws, does not have similar requirements around the handling of the associated data. The *Privacy and Personal Information Protection Act 1998* (NSW) establishes Information Privacy Principles similar to Victoria's Privacy and Data Protection Act, but again the Act only applies to public sector organisations.[48]

Similarly, Queensland's *Information Privacy Act 2009* (Qld) sets up privacy obligations for government departments, public sector agencies and contractors. Queensland also has a human rights charter that protects individuals from arbitrary interference with their privacy, and like in Victoria and the ACT, the charter requires public authorities to act in a way that is compatible with the rights within it.[49]

In the Northern Territory, the *Information Act 2002* (NT) sets out Information Privacy Principles for public sector agencies. Western Australia, South Australia and Tasmania do not have overarching privacy legislation, but there are some privacy provisions split up across other laws such as health legislation that protects health information. South Australia's Department of Premier and Cabinet has issued an Information Privacy Principles Instruction.[50]

FINDING 25: The Australian Capital Territory is the only Australian jurisdiction that regulates the handling of workplace surveillance data, making it an offence for employers to fail to protect records from misuse, loss and unauthorised access, modification or disclosure, and to fail to destroy or de-identify records that are no longer needed.

---

46 *Workplace Privacy Act 2011* (ACT) s 44.

47 Tasmania Law Reform Institute, *Review of privacy laws in Tasmania*, final report, no. 33, Hobart, May 2024, p. 201.

48 Ibid., p. 199.

49 Ibid., pp. 199–200.

50 Ibid., pp. xi, 200.

5.2.3 Employee records and small businesses are exempt from the federal Privacy Act

As discussed in previous chapters, the *Privacy Act 1988* (Cth) protects the privacy of Australians by outlining how their personal information should be handled by the public sector and organisations with an annual turnover greater than $3 million. It does this by setting out 13 Australian Privacy Principles (APPs) that are similar to the Victorian IPPs. However, there are significant gaps in privacy protection for workers' data. For example, the Privacy Act does not apply to:

- small businesses with an annual turnover of $3 million or less
- registered political parties
- media organisations
- employee records of current and former employees
- an act or practice directly related to the employment relationship between an employer and an individual.[51]

These exemptions coupled with the exclusion of the private sector from the Victorian Privacy and Data Protection Act means that there is no privacy regulation for a significant amount of Victorian employees' personal records, especially considering over 90% of small businesses in Australia have a turnover of less than $2 million.[52] A recent review of the federal Privacy Act has recommended removing these exemptions, but these changes are yet to occur.[53]

The exclusion of employee records that relate to a current or former employment relationship between an employee and employer eliminates any constraints on how employers handle surveillance data and minimises privacy protection of workers' personal information.[54] The exemption of employee records was originally included because they were seen to be a matter best dealt with by workplace relations legislation that at the time was governed by state and territory laws.[55]

Furthermore, the broad interpretation of 'employee records' means that there is a high threshold in terms of what information falls under the Privacy Act's protections.[56] For example, courts have deemed an entire computer issued by an employer to be an employee record meaning that none of the information held in that computer

---

51 *Privacy Act 1998* (Cth) ss 6C, 6D, 7B, 7C.

52 Centre for Decent Work and Industry, *Submission 13*, p. 12; National Tertiary Education Union, *Submission 24*, p. 14; Office of the Victorian Information Commissioner, *Submission 39*, p. 3; Australian Industry Group, *Submission 40*, p. 16; Associate Professor Alysia Blackham, *Transcript of evidence*, p. 36; Heap, *No blood—no job*, p. 10; Australian Bureau of Statistics, *Counts of Australian businesses, including entries and exits*, 2023, <https://www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/jul2019-jun2023> accessed 22 November 2024.

53 Office of the Victorian Information Commissioner, *Submission 39*, p. 3; Associate Professor Alysia Blackham, *Transcript of evidence*, p. 36.

54 National Tertiary Education Union, *Submission 24*, p. 12; Australian Manufacturing Workers' Union, *Submission 31*, p. 16.

55 Attorney-General's Department, *Privacy Act review*, p. 64.

56 Australian Nursing and Midwifery Federation, *Submission 38*, p. 12; Attorney-General's Department, *Privacy Act review*, p. 65.

is subject to privacy protection.[57] Courts have also generally accepted employers' surveillance practices that otherwise would be an infringement of privacy, so long as the surveillance has been used to demonstrate a breach of conduct and it does not unreasonably collect other types of sensitive information.[58]

The different exemptions based on business size, what classifies as an employee record and which acts and practices are related to the employment relationship undermine the efficacy of the Privacy Act's protections, create confusion and uncertainty for both employers and employees, and leave a significant amount of workers' personal information unprotected.[59]

A review of the Privacy Act, which considered whether the Act and its enforcement mechanisms were currently fit for purpose, was completed by the Attorney-General's Department in 2022. It stated that, '[c]urrent exemptions from the Act require recalibration to address contemporary privacy risks and meet current community expectations.'[60] It also found that entities should ensure that their information-handling practices are fair and cause no harm, there should be greater privacy protections around personal information in high-risk circumstances, and individuals need more transparency and control around how their information is handled. It also supported strengthening enforcement of privacy obligations and enabling individuals to seek redress for privacy breaches in the courts.[61]

To meet community expectations, the report proposed that the Act cover small businesses in the future following an impact analysis, extensive consultation with small businesses and the development of appropriate supports. In the meantime, it recommended making small businesses that trade in personal information and small businesses that use facial recognition technology exceptions to the small business exemption.[62] Other proposals included introducing a statutory tort for serious invasions of privacy, a 'fair and reasonable' test to underpin how entities handle personal information, and requirements for entities to establish and periodically review data retention timeframes and to conduct a privacy impact assessment before commencing an activity that could have a significant impact on an individual's privacy.[63]

In its response to the review's 116 proposals, the Australian Government agreed to 38 proposals, agreed in principle to 68 and noted 10.[64] As discussed in chapters 1 and 4, the first tranche of reforms to the Privacy Act were passed in December 2024; however, they do not substantially change how the privacy of workplace surveillance data is protected.

---

57 Associate Professor Alysia Blackham, *Transcript of evidence*, p. 39.

58 National Tertiary Education Union, *Submission 24*, p. 14.

59 Heap, *No blood—no job*, p. 11.

60 Attorney-General's Department, *Privacy Act review: report on a page*, factsheet, Australian Government, Canberra, February 2023, p. 1.

61 Ibid.

62 Attorney-General's Department, *Privacy Act review*, pp. 2, 6.

63 Ibid., pp. 3, 15.

64 Australian Government, *Government response: Privacy Act review report*, Canberra, 2023, p. 2.

FINDING 26: Exemptions for small businesses and employee records in the *Privacy Act 1988* (Cth) mean a significant amount of Victorian employees' personal information does not have privacy protection.

There are also limited protections around the privacy of employees' personal information in the *Fair Work Act 2009* (Cth). While under the Act employers are required to ensure the accuracy of records they must hold to comply with workplace laws and ensure the confidentiality of information concerning requests for leave, there are no provisions to protect the data collected by workplace surveillance and how it is handled.[65]

5.2.4 The European Union has robust data protection laws

The European Union (EU) has robust privacy and data protection laws.[66] Article 8(1) of the EU Charter of Fundamental Rights gives individuals the right to personal data protection. Any organisation (whether based in the EU or elsewhere) that is established in the EU or processes the data of an EU citizen must comply with the data processing rules set out in the EU's General Data Protection Regulation (GDPR).[67] The GDPR has seven key principles relating to the processing of personal data and provides individuals information privacy rights. The principles are:

- lawfulness, fairness and transparency—data is processed lawfully, fairly and in a transparent manner
- purpose limitation—data is collected for specified, explicit and legitimate purposes and only processed for these purposes
- data minimisation—data collection is limited to what is necessary to achieve the stated purpose
- accuracy—collected data is accurate and kept up to date
- storage limitation—collected data is kept in an identifiable form for no longer than is necessary
- integrity and confidentiality—data is processed in a secure manner
- accountability—entity collecting the data is responsible for, and must be able to demonstrate, compliance with these principles.[68]

---

65 Australian Manufacturing Workers' Union, *Submission 31*, p. 9; The Centre for Future Work, *Submission 32*, pp. 4–5; Murray Brown and Chris Dent, 'Privacy concerns over employer access to employee social media', *Monash University Law Review*, vol. 43, no. 3, 2017, p. 819.

66 Victorian Government, *Submission 43*, p. 10; Eurofound, *Employee monitoring and surveillance: the challenges of digitalisation*, Publications Office of the European Union, Luxembourg, 2020, p. 7.

67 European Union, *General Data Protection Regulation*, 2018, <https://gdpr-info.eu> accessed 3 February 2025.

68 Ibid.

The GDPR affords individuals the right to:

- access their information
- rectify their information
- request deletion of their information
- restrict processing of their data
- have their data transmitted to another entity
- object to the processing of their data
- be notified of a data breach
- not be subject to automated decision-making and profiling.[69]

The United Kingdom (UK) has similar laws regarding data protection rights. The UK GDPR and *Data Protection Act 2018* (UK) obligate employers to protect the personal information they handle in employee records and recruitment and selection records.[70]

Despite not explicitly addressing workplace surveillance, many stakeholders referred the Committee to the EU's GDPR as an overseas example of best-practice data protection regulation that has informed privacy standards worldwide.[71] They noted the GDPR emphasises legitimacy, transparency and proportionality, imposes significant fines on non-compliant businesses and enables individuals to challenge processing practices and seek compensation if their data has been mishandled.[72] EU member states are bound by the GDPR, which are enforced by national data protection authorities. EU countries can also choose to develop more specific workplace surveillance regulation.[73] For example, Finland has a strict necessity requirement for workplace surveillance, where it can only be conducted to protect health, safety or property.[74]

Other examples of international regulation of personal data include Canada's *Personal Information Protection and Electronic Documents Act* (S.C. 2000 c. 5) which governs the collection, use and disclosure of personal information by private sector organisations and federally regulated entities such as banks, airlines and

---

69 Ibid.; Office of the Victorian Information Commissioner, *EU general data protection regulation*, 2020, <https://ovic.vic.gov.au/privacy/resources-for-organisations/eu-general-data-protection-regulation> accessed 16 May 2024.

70 Victorian Government, *Submission 43*, p. 10; Information Commissioner's Office UK, *Overview—data protection and the EU*, (n.d.), <https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu> accessed 3 February 2025.

71 For example, Australian Lawyers Alliance, *Submission 7*, p. 10; Master Electricians Australia, *Submission 11*, p. 8; Professor Peter Holland and Dr Jacqueline Meredith, *Submission 22*, p. 13; Australian Services Union, Victorian and Tasmanian Authorities and Services Branch, *Submission 29*, p. 8; Australian Nursing and Midwifery Federation, *Submission 38*, p. 10; Victorian Government, *Submission 43*, p. 10; James Fleming, Executive Director, Australian Institute of Employment Rights, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, pp. 3–4; Dr Jacqueline Meredith, Lecturer, Swinburne Law School, Swinburne University of Technology, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, pp. 5–6.

72 Australian Lawyers Alliance, *Submission 7*, p. 11; Master Electricians Australia, *Submission 11*, p. 8; Alysia Blackham, 'Setting the framework for accountability for algorithmic discrimination at work', *Melbourne University Law Review*, vol. 47, no. 63, 2023, pp. 81–82.

73 Eurofound, *Employee monitoring and surveillance*, p. 7.

74 Dr Jacqueline Meredith, *Transcript of evidence*, p. 6.

telecommunications companies. It has a similar set of data protection principles as the GDPR, including legitimacy, proportionality, transparency, data minimisation, accuracy, access and accountability.[75] Similarly, the *Federal Data Protection Act* (Germany) 30 June 2017 obliges German businesses to ensure their data processing is fair, legitimate, honest and transparent, and the *California Consumer Privacy Act of 2018* gives private sector workers the right to know when and why they are being monitored, to access their data and request correction or deletion, and opt out of employers selling their data.[76]

While the introduction of the GDPR in 2018 increased awareness of data protection among employers and employees in the EU, some employers find the legislation too imprecise to provide certainty around how to comply with the regulations. Critics have also stated that the GDPR's focus on information privacy makes it a limited tool for regulating workplace surveillance, its flexible application between EU member states creates uncertainty and competition between countries, and it does not set clear limitations on specific surveillance technologies.[77]

Associate Professor Normann Witzleb from Monash University's Faculty of Law and The Chinese University of Hong Kong's Faculty of Law told the Committee he was wary of advocating a wholesale adoption of the GDPR in Victoria because it would clash with federal privacy laws and create too much complexity. Instead, Victoria should use it as a reference point when considering how to better regulate the protection of surveillance data.[78]

5.2.5 The International Labour Organization guides the protection of workers' data

As discussed in Chapter 4, Australia has ratified the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, both of which recognise individuals' right to privacy. While no international conventions specifically cover workplace surveillance, the International Labour Organization has a non-binding Code of Practice on the Protection of Workers' Personal Data. Despite having no binding force, this Code of Practice published in 1997 makes recommendations on how to process workers' personal data in a manner that protects workers' rights, dignity

---

75 Leonard, 'Workplace surveillance and privacy', pp. 63–64; Australian Lawyers Alliance, *Submission 7*, p. 11.

76 *California Consumer Privacy Act of 2018* [1798.105, 1798.106, 1798.110, 1798.130]; Australian Lawyers Alliance, *Submission 7*, p. 11; Victorian Government, *Submission 43*, p. 11.

77 National Tertiary Education Union, *Submission 24*, p. 15; Joanna Bronowicka, et al., *'Game that you can't win'?: workplace surveillance in Germany and Poland*, European University Viadrina, Frankfurt, 2020, pp. 29–31; Paul De Hert and Georgios Bouchagiar, 'Visual and biometric surveillance in the EU. Saying 'no' to mass surveillance practices?', *Information Polity*, vol. 27, no. 2, 2022, pp. 197, 206–208.

78 Associate Professor Normann Witzleb, Faculty of Law, Monash University, and Faculty of Law, The Chinese University of Hong Kong, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 44.

and privacy.[79] Some of the principles relevant to workplace surveillance and this Inquiry include:

- Personal data should be processed lawfully and fairly, and only for reasons directly relevant to the employment of the worker.
- Personal data should, in principle, be used only for the purposes for which it was originally collected.
- Decisions concerning a worker should not be based solely on the automated processing of that worker's personal data.
- Personal data collected by electronic monitoring should not be the only factor in evaluating worker performance.
- Workers and their representatives should be kept informed of any data collection process, the rules that govern that process, and their rights.
- Workers may not waive their privacy rights.
- Statements seeking consent to collect or disclose workers' information must be in plain language and specify the data to be disclosed, why the data will be collected and how long the statement remains valid.
- Employers should not collect data about a worker's sex life, religious or political beliefs, criminal history or trade union membership unless allowed by law.
- Workers should have advance notice of workplace monitoring, the methods used, the time schedule and what data will be collected.
- Employers should keep personal data safe from loss and unauthorised access, use, modification or disclosure.
- Data should only be stored for as long as it is needed.
- Workers should have access to all their personal data.
- Workers' representatives should be consulted about the introduction or modification of an automated system that processes workers' personal data and the introduction of any electronic monitoring of workers' behaviour in the workplace.[80]

5.2.6 Best-practice data protection is transparent and accountable

The EU's GDPR is commonly raised as a best-practice example of data protection regulation, with its focus on transparency, proportionality, data minimisation and accountability.[81] The Organisation for Economic Co-operation and Development

---

79 International Labour Organization, *Protection of Workers' Personal Data: an ILO code of practice*, International Labour Office, Geneva, 1997, p. 1.

80 Ibid., pp. 2–7; Victorian Trades Hall Council, *Submission 28*, p. 37.

81 Australian Lawyers Alliance, *Submission 7*, p. 10; Attorney-General's Department, *Privacy Act review*, p. 3; Kirstie Ball, *Electronic monitoring and surveillance in the workplace: literature review and policy recommendations*, Publications Office of the European Union, Luxembourg, 2021, pp. 71–72.

also has a set of privacy principles that echo the GDPR principles; namely, collection limitation, data quality, purpose specification, use limitation, openness, individual participation and accountability.[82]

The Australian HR Institute presented the Committee with examples of best practice data protection such as developing comprehensive and accessible data management policies, establishing timeframes for data retention and destruction, ensuring third parties handling data meet safety standards, restricting access to authorised personnel, regularly auditing surveillance data to detect vulnerabilities in the types of data collected, continuously monitoring and updating security measures, and educating employees on surveillance practices, policies and data protection.[83]

The Fair Work Ombudsman has developed a best practice guide for employers on workplace privacy. It specifies that best-practice employers tell their employees, even when not obliged to by law, what personal information they collect and why, who that information might be disclosed to and how employees can access their information and correct it if necessary. It also recommends employers develop a workplace privacy policy and train managers and employees about workplace privacy.[84]

As discussed in Chapter 4, the UK Information Commissioner's Office (ICO), which upholds information and data privacy rights for individuals, produces guidance on data protection and monitoring workers based on the UK GDPR. Some of its best-practice guidelines for employers around data protection include informing workers what personal information is being collected and why, updating them if there are any changes and ensuring any data gathered through surveillance is not incorrect and misleading, and correcting or erasing it if it is, especially if the information is used to make potentially adverse decisions about employees.[85]

FINDING 27: The European Union's General Data Protection Regulation that lists seven key principles for the processing of personal data and sets out individuals' data privacy rights is considered internationally as best-practice regulation for information privacy.

5.3 Data protection in Victoria can be strengthened

As explained in Section 5.2, gaps in current state and federal legislation do not adequately protect employees' privacy and workplace surveillance data. OVIC told the Committee that Victoria's Privacy and Data Protection Act 'must be amended to sufficiently regulate Victorian public sector (VPS) entities' use of workplace surveillance.'[86] This section outlines how data protection regulation can be strengthened in Victoria. It first addresses the potential impact of reforms to the

82 Ball, *Electronic monitoring and surveillance in the workplace*, p. 72.

83 Australian HR Institute, *Submission 10*, p. 4.

84 Fair Work Ombudsman, *Workplace privacy best practice guide*, pp. 6–8.

85 Information Commissioner's Office UK, *Employment practices and data protection: monitoring workers*.

86 Office of the Victorian Information Commissioner, *Submission 39A*, p. 2.

federal Privacy Act on Victorian workplaces before recommending specific ways to expand privacy protections around Victorian employees' personal information. It concludes by considering the role of an oversight body to regulate workplace surveillance and data protection.

5.3.1 The first round of Privacy Act reforms do not alter how employee data is treated

Business groups recommended the Committee withhold any proposed changes to workplace surveillance regulation until there is greater clarity around proposed amendments to the Privacy Act. They suggested the Committee limit any changes to non-binding best-practice guidelines to reduce the risk of legislative overlap that could lead to ambiguity and extra red tape.[87]

The first tranche of Privacy Act reforms was introduced to the federal parliament in September 2024 and was passed in December 2024. The reforms introduced a statutory tort for serious invasions of privacy, which enables individuals to commence proceedings in court and seek compensation for serious violations of their privacy. This may protect workers in some instances but only if they can prove they had a reasonable expectation of privacy and the invasion of privacy was intentional or reckless.[88] There will also be a requirement beginning in December 2026 for greater transparency around automated decision-making that is reached using individuals' personal information, which could address concerns about the opaque nature of artificial intelligence and algorithms using workplace surveillance data to make employment decisions.[89]

However, more significant Privacy Act reforms that were anticipated such as the removal of exemptions for employee records and small businesses did not eventuate. These reforms would have had a substantial impact on how employers monitor employees and treat workplace surveillance data. The removal of these exemptions had the support of the Australian Law Reform Commission, the Attorney-General's Department and the Office of the Australian Information Commissioner (OAIC), which regulates compliance with the Privacy Act, because their current inclusion lacks justification, does not meet community expectations and conflicts with overseas data protection regimes such as the GDPR.[90]

---

87 Victorian Automobile Chamber of Commerce, *Submission 26*, p. 11; Australian Industry Group, *Submission 40*, pp. 29–30; Scott Barklamb, Principal Advisor, Workplace Relations Policy, Australian Industry Group, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, pp. 33, 36; Amelia Bitsis, Executive Director, Policy and Advocacy, Victorian Chamber of Commerce and Industry, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 19.

88 Privacy and Other Legislation Amendment Bill 2024 (Cth) Schedule 2, Part 2, cl 7.

89 Geoff McGrath, et al., *Australia's first tranche of privacy reforms: a deep dive and why they matter*, Ashurst, 2024, <https://www.ashurst.com/en/insights/australias-first-tranche-of-privacy-reforms-a-deep-dive-and-why-they-matter> accessed 23 January 2025.

90 Murray Brown and Normann Witzleb, 'Big brother at work: workplace surveillance and employee privacy in Australia', *Australian Journal of Labour Law*, vol. 34, no. 3, 2021, p. 28; Chen and John Howe, *Worker data right*, p. 7; Heap, *No blood—no job*, p. 27.

If the exemptions were abolished and the Privacy Act applied to employee data, the collection, storage, access and use of workplace surveillance data would be subject to the APPs requiring employers to collect data in a manner that is fair and proportionate and to only collect and use the data for a specified, legitimate purpose.[91] As it stands, the first tranche of Privacy Act reforms falls short of protecting employees' information privacy and it is unlikely that a second tranche of reforms will be introduced before the 2025 federal election. This heightens the need for Victoria to strengthen regulation to protect employees' data.[92]

FINDING 28: Recent changes to the *Privacy Act 1988* (Cth) do not address shortcomings in how employees' personal information is protected and, since further changes are not expected in the near future, this reinforces the need for Victoria to strengthen data protection regulation.

5.3.2 Expanding Victoria's privacy protections will reduce data security risks

As recommended in Chapter 4, requiring employers to ensure any workplace surveillance is reasonable, proportionate and necessary for achieving a legitimate purpose, along with obliging them to notify, disclose details and consult with workers about the surveillance, will minimise the risk of workplace surveillance intruding on employees' privacy. It will encourage employers to clarify the purpose for which they are collecting the data and help them to determine when to destroy the data.[93]

Additional protections on how workplace surveillance data is used, stored, shared and disposed of will reduce the associated data security risks discussed in Section 5.1.2. This section proposes several additional privacy protections that Victoria could implement to strengthen data protection for workers in the state. These recommendations can sit alongside any future amendments to the Privacy Act that may remove exemptions for small businesses and employee records.

According to Professor Peter Leonard, a lawyer who works in the privacy and data security space:

> there are four common problems in relation to the [data] practices of organisations. There is overcollection of information; there is overexposure of information within an organisation—that is, they do not put enough controls in place as to who can see what information and in what circumstances; the third problem is overuse, which partly flows from overexposure; and the other is over-retention—too many organisations

91 Brown and Witzleb, 'Big brother at work', p. 28.

92 Danae Fleetwood, Master of Philosophy research student, Centre for Decent Work and Industry, QUT, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 21.

93 Office of the Victorian Information Commissioner, *Submission 39A*, p. 8; Blackham, 'Surveillance, data collection and privacy at work', p. 7.

retain information far longer than they need to retain it for the purpose for which it was collected.[94]

He told the Committee that the problem with most modern data privacy and surveillance laws is that they rely on the individual whose data is being collected to engage with notices of collection and decide how to respond, when most people do not have the time or technical understanding to engage with these notices. Instead, the organisation collecting the data should be accountable for ensuring that the data it collects is for a specific, legitimate purpose and that it is only used and accessed in appropriate circumstances.[95] Dr Fiona Macdonald, a Policy Director with the Australia Institute's Centre for Future Work, agreed, stating that making employers accountable for how they collect, use and store workplace surveillance data rather than relying on employees to assess data handling practices after the fact would be the preventative and preferred approach.[96]

The Committee also heard that Victoria should implement a number of protective measures to match the information privacy rights provided by the GDPR such as individuals' right to access their data in a form they can use, to have their data erased and to be able to challenge how their data is collected and used by appealing to a regulator.[97] The GDPR's restriction on only collecting data that is strictly necessary and limiting the collection of sensitive information to specific circumstances would help with data minimisation.[98] Furthermore, establishing penalties for data misuse similar to the GDPR would keep employers accountable.[99] The Committee also heard that if employees have the ability to see what data their employer is holding, how they are storing it and for how long, then employers will think twice about the appropriateness of their data handling practices.[100]

Stakeholders also supported data minimisation, development of retention policies, encryption of data for transmission, storage and processing, and vetting third-party surveillance providers against data security and compliance standards.[101] Unions requested consultation with workers about data handling practices, requiring employers to undertake privacy impact assessments to identify the risks associated with handling surveillance footage, banning employers from on-selling workers' data to third parties and limiting the collection of sensitive personal information to when it is strictly necessary or required by law.[102]

---

94 Professor Peter Leonard, Principal, Data Synergies and Professor of Practice, UNSW Business School, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 7.

95 Ibid., pp. 6, 7.

96 Dr Fiona Macdonald, Policy Director, Industrial and Social, Centre for Future Work, Australia Institute, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 21.

97 James Fleming, *Transcript of evidence*, pp. 3–4.

98 Heap, *No blood—no job*, pp. 23, 24.

99 James Fleming, *Transcript of evidence*, pp. 2–3.

100 Professor Peter Holland, *Transcript of evidence*, p. 8; Dr Jacqueline Meredith, *Transcript of evidence*, p. 8.

101 Dr Jean Linis-Dinco, *Submission 6*, p. 1; Australian Lawyers Alliance, *Submission 7*, p. 7; Australian Security Industry Association Limited, *Submission 21*, pp. 4, 5; Australian Manufacturing Workers' Union, *Submission 31*, p. 23.

102 United Workers Union, *Submission 25*, pp. 19–20; Victorian Trades Hall Council, *Submission 28*, pp. 17, 35; Australian Nursing and Midwifery Federation, *Submission 38*, p. 13; Kat Hardy, Lead Organiser, Australian Services Union, Victorian Private Sector Branch, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 47.

The recent Inquiry into the digital transformation of workplaces, tabled in February 2025 by the Australian House of Representatives Standing Committee on Employment, Education and Training and discussed further in Chapter 1, recommended the Australian Government review the Fair Work Act and Privacy Act to prohibit the sale of workers' personal information and any data collected in the course of work to third parties. It also recommended a ban on high-risk uses of workers' data such as disclosure to technology developers to develop AI systems.[103]

In this current Inquiry, OVIC suggested the Committee base Victorian workplace surveillance law reform around requiring employers to document a clear, specific purpose for a workplace surveillance activity and supply this to employees. This becomes a mechanism of accountability for employers, ensuring the gathered data cannot be used for an unrelated purpose, without restricting workplace surveillance activities. OVIC suggested this be incorporated into the Privacy and Data Protection Act.[104]

OVIC also suggested that a new IPP be introduced to the Act to embed privacy into the design of a workplace surveillance activity. The new IPP would place a positive obligation on organisations to ensure they comply with the IPPs. This would mimic APP 1.2 in the federal Privacy Act and, in terms of workplace surveillance, it 'would require employers to have systems, procedures and processes in place that govern a workplace surveillance activity.'[105]

Prohibiting employers from selling workers' personal information to third parties would better protect employees' data privacy. Employers should also have mechanisms in place, such as regular audits, to ensure that any third party that is collecting or storing workplace surveillance data on their behalf is complying with legal requirements and the employer's policies around data storage, security and retention.

RECOMMENDATION 9: That the Victorian Government include a requirement in new workplace surveillance legislation that employers must inform employees who is collecting workplace surveillance data, how the data is secured, stored and disposed of, who can use the data and for what purpose, and how long the data will be kept.

RECOMMENDATION 10: That the Victorian Government include a provision in new workplace surveillance legislation that employers must not sell employees' personal data, or any data collected about employees through surveillance, to a third party.

---

103 Parliament of Australia, House of Representatives Standing Committee on Employment, Education and Training, *The future of work: Inquiry into the digital transformation of workplaces*, February 2025, p. 58.

104 Office of the Victorian Information Commissioner, *Submission 39A*, p. 7.

105 Ibid., p. 4.

RECOMMENDATION 11: That the Victorian Government include a requirement in new workplace surveillance legislation that employers must ensure that any third party they contract to collect or store workplace surveillance data takes reasonable steps to protect the data and complies with the employers' workplace surveillance policy.

RECOMMENDATION 12: That the Victorian Government amend the *Privacy and Data Protection Act 2014* (Vic) to introduce a new Information Privacy Principle, modelled on Australian Privacy Principle 1.2, that places a positive obligation on organisations and employers to ensure they comply with the Information Privacy Principles.

Workers should be able to access data generated about them from surveillance

Another theme in the evidence was the importance of employees having access to data generated about them from workplace surveillance.[106] As the Victorian Information Commissioner Sean Morrison told the Committee:

> people should have access to this information, especially if it is being used for a disciplinary or lawful purpose against them. We say this is a fundamental protection in the balance of power between employers and employees.[107]

There is no legislation stating that employees are entitled to access this data and the evidence received suggested this data is being withheld from employees. For example, the NTEU survey found that 41% of respondents said they could not access data their employers collect on them and 56% were unsure of how to access this data.[108] The Committee also heard more specific examples such as employers withholding CCTV footage from employees who wish to use it to support a bullying or sexual harassment claim.[109]

The Australian Lawyers Alliance, a national association of lawyers, academics and other professionals dedicated to protecting the rights of the individual, also mentioned instances where employers have refused employees' requests to access workplace surveillance data in the context of workers' compensation claims, or where employers use this data to dispute a compensation claim without sharing this evidence with employees. Withholding this data can delay claims, add to costs, create additional complications and stress, and compromise injured employees' access to justice.[110]

---

106 Victorian Trades Hall Council, *Submission 28*, p. 35; Australian Education Union, *Submission 42*, p. 1; Chris Molnar, Co-Chair, LIV Workplace Relations Committee, Law Institute of Victoria, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 25; James Fleming, *Transcript of evidence*, p. 3.

107 Sean Morrison, *Transcript of evidence*, p. 11.

108 National Tertiary Education Union, *Submission 24*, p. 12.

109 Australian Lawyers Alliance, *Submission 7*, p. 8; United Workers Union, *Submission 25*, p. 9; Nicole McPherson, *Transcript of evidence*, p. 47.

110 Australian Lawyers Alliance, *Submission 7*, p. 8; Sha Hotchin, Secretary, Victoria Branch Committee, Australian Lawyers Alliance, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 26.

Other circumstances where employees are denied access to workplace surveillance data are in disciplinary processes and workplace incident investigations. Several unions told the Committee that employers are relying on surveillance data such as CCTV footage in these situations, but employees are not able to review this evidence and provide context and explanation. They claimed this was a 'breach of justice' and that employers should be obligated to provide employees access to this data in these circumstances.[111]

Susan Accary, Victoria Branch Committee President of the Australian Lawyers Alliance, advocated for employers to promptly give employees or their representatives access to workplace surveillance data in the case of a dispute to progress claims swiftly, which is in the interests of both employers and employees.[112] Similarly, Dr Macdonald from the Centre for Future Work told the Committee:

> If decisions are being made on the basis of data, then employees should know what that data is. Where data is used to impact on employees, employees should have access to that data.[113]

Amy Salmon, Principal Psychological Health and Safety Specialist at WorkSafe Victoria, the state's workplace health and safety authority, cautioned that providing such access could compromise the privacy of other individuals captured in the data.[114] However, individuals' access to data held about them is recognised by best-practice data protection regulation. For instance, it is an explicit right in the GDPR, and the ACT's Workplace Privacy Act also requires employers to allow employees access to data generated about them from workplace surveillance upon written request by the employee.[115] If an employer refuses, then that data cannot be used in legal proceedings or to take adverse action against the worker.[116]

RECOMMENDATION 13: That the Victorian Government include a requirement in new workplace surveillance legislation that employers, upon request by an employee, must give the employee access to workplace surveillance data generated about the employee.

---

111 Karen Batt, Secretary, Community and Public Sector Union, Victorian Branch, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 47; Tash Wark, Secretary, Australian Services Union, Victorian and Tasmanian Authorities and Services Branch, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 48; Jenny Kruschel, National Secretary, Textile Clothing Footwear, Manufacturing Division, Construction, Forestry and Maritime Employees Union, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 53; Paris Nicholls, *Transcript of evidence*, p. 54; Australian Nursing and Midwifery Federation, Victorian Branch, *Hearing notes*, supplementary evidence received 1 November 2024, p. 2.

112 Susan Accary, President, Victoria Branch Committee, Australian Lawyers Alliance, public hearing, Melbourne, 23 September 2024, *Transcript of evidence*, p. 26.

113 Dr Fiona Macdonald, *Transcript of evidence*, p. 21.

114 Amy Salmon, Principal Psychological Health and Safety Specialist, WorkSafe Victoria, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 24.

115 European Union, *General Data Protection Regulation*; *Workplace Privacy Act 2011* (ACT) s 23.

116 *Workplace Privacy Act 2011* (ACT) s 23.

Biometric data must be considered as sensitive personal information

As discussed in Section 5.1.2, biometric data is highly sensitive and cannot be replaced or changed in the event of a data breach, potentially resulting in devastating and ongoing ramifications through identity fraud.[117] Best-practice data protection regulation limits the collection of biometric data to a legitimate purpose, which cannot be achieved in a less intrusive manner, and which is balanced against an individual's privacy and the potential for discrimination.[118] The Committee heard there are concerns about organisations collecting and using biometric data as routine practice such as for gaining access to workplace premises, rather than for reasons directly related to job requirements such as assessing fitness to work.[119]

Section 5.2.1 also mentioned how unlike the federal Privacy Act, the Victorian Privacy and Data Protection Act does not include biometric data in the definition of sensitive information.[120] OVIC claimed that it was critical for this definition to change to deem biometric data as sensitive information to 'require employers to satisfy additional criteria before implementing biometric surveillance in the workplace' such as ensuring collection is proportionate to the purpose and employees have given consent.[121] This would also make Victorian legislation consistent with federal and international privacy laws.[122]

According to Sean Morrison, changing the definition of sensitive information to include biometric data in the Privacy and Data Protection Act is only 'the first fix' and tighter controls should also be implemented such as requiring employers to conduct a privacy impact assessment and security impact assessment to identify and mitigate privacy and data security risks around biometric data.[123] Adjunct Professor Moira Paterson from the Castan Centre for Human Rights Law at Monash University suggested that Victoria embed further protections for biometric data in dedicated workplace surveillance laws to cover all employers not just the public sector.[124]

RECOMMENDATION 14: That the Victorian Government amend the *Privacy and Data Protection Act 2014* (Vic) to include biometric data in the definition of sensitive information.

---

117 Office of the Victorian Information Commissioner, *Submission 39A*, p. 3; Sean Morrison, *Transcript of evidence*, p. 11.

118 Heap, *No blood—no job*, p. 29.

119 Ibid.; Centre for Decent Work and Industry, *Submission 13*, p. 6; United Workers Union, *Submission 25*, p. 18.

120 Office of the Victorian Information Commissioner, *Privacy during employment*; Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 47.

121 Office of the Victorian Information Commissioner, *Submission 39A*, p. 3; Rachel Dixon, Privacy and Data Protection Deputy Commissioner, Office of the Victorian Information Commissioner, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 16.

122 Office of the Victorian Information Commissioner, *Submission 39*, p. 6.

123 Sean Morrison, *Transcript of evidence*, p. 15.

124 Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 47.

RECOMMENDATION 15: That the Victorian Government through new workplace surveillance legislation restrict employers from collecting and using employees' biometric data to circumstances where there is a legitimate purpose that cannot be achieved through less intrusive means.

Victoria should introduce a mandatory data breach notification scheme

Another gap in the Victorian Privacy and Data Protection Act is the absence of a requirement for VPS organisations to report information security incidents such as a data breach to affected individuals. This means that individuals whose data has been misused, lost or accessed without authorisation may not ever be told so they can take remedial action such as change their password or cancel a card.[125] While there are requirements for VPS organisations to report certain information security incidents to OVIC, they do not:

- cover all information security and privacy incidents
- require that affected individuals be notified
- apply to all VPS organisations.[126]

This is inconsistent with the federal Privacy Act, which requires entities to notify individuals and the OAIC when a data breach is likely to cause serious harm to an affected individual. NSW has a similar requirement for public sector organisations, as will Queensland by July 2025.[127] OVIC supported amending the Privacy and Data Protection Act to introduce a mandatory incident notification scheme.[128]

Despite the Privacy Act protecting consumers who are affected by a data breach, workers do not have similar protections. The Attorney-General Department's review of the Privacy Act noted that many of its submitters called for extending this protection to the workplace.[129] It proposed that privacy protection for private sector employees be enhanced through 'notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm' and that further consultation with employer and employee representatives was needed to determine how this could be incorporated into legislation.[130]

Considering the amount, range and sensitivity of the data employers collect about their employees for human resources and remuneration purposes and through workplace surveillance, the lack of protection for workers in the event of a data breach in either state or federal legislation is a significant gap.

---

125 Office of the Victorian Information Commissioner, *Submission 39A*, pp. 3–4.

126 Ibid.

127 Ibid., p. 3.

128 Ibid., p. 2.

129 Attorney-General's Department, *Privacy Act review*, p. 68.

130 Ibid., p. 71.

RECOMMENDATION 16: That the Victorian Government amend the *Privacy and Data Protection Act 2014* (Vic) to introduce a mandatory incident notification scheme that requires organisations to inform affected individuals and the Office of the Victorian Information Commissioner of a data breach.

IPP protection should extend to private sector employees

As discussed throughout this chapter, there are large gaps in state and federal legislation that leave private sector employees without protection in terms of their data and privacy. This is an issue that was raised as far back as 2005 when the Victorian Law Reform Commission reviewed state workplace surveillance regulation, and suggested that if the employee records exemption is retained in the Privacy Act, Victoria should extend information privacy protections to the private sector to protect all employees' data.[131]

Another gap highlighted by OVIC and referred to in the previous subsection about data breaches is that not all VPS organisations that fall under the Privacy and Data Protection Act must meet the requirements of IPP 4, which obliges organisations to protect the personal information they hold from misuse, loss and unauthorised access, modification or disclosure and requires them to destroy or permanently de-identify data they no longer need. The exempt organisations include public hospitals, universities and councils. OVIC called for IPP 4 to apply to these currently exempt entities.[132]

However, this still leaves Victorian private sector employees without data privacy protections. OVIC recognised that while its proposed changes would be 'sufficient to regulate VPS entities' use of workplace surveillance', it would leave private sector employees unprotected.[133] A potential solution would be to amend the Privacy and Data Protection Act to require employers who engage in a workplace surveillance activity to comply with the IPPs.[134] Introducing this requirement could place a burden on smaller businesses that may not have the 'resources or corporate knowledge to engage with the IPPs', but as discussed in Chapter 4, smaller businesses are less likely to use intrusive surveillance technologies and employees of small businesses deserve similar protections to those afforded to VPS employees.[135]

RECOMMENDATION 17: That the Victorian Government extend the privacy protections embedded in the *Privacy and Data Protection Act 2014* (Vic) to employees in all sectors by requiring employers operating in Victoria who engage in a workplace surveillance activity to comply with the Information Privacy Principles.

---

131 Victorian Law Reform Commission, *Workplace privacy: final report*, Melbourne, 2005, p. 10.

132 Office of the Victorian Information Commissioner, *Submission 39A*, pp. 2–3.

133 Ibid., p. 4.

134 Sean Morrison, *Transcript of evidence*, p. 14; Office of the Victorian Information Commissioner, *Submission 39A*, p. 4.

135 Office of the Victorian Information Commissioner, *Submission 39A*, p. 4.

5.3.3 A regulator should be appointed to oversee workplace surveillance

Stakeholders spoke of the need for Victoria to appoint an independent regulator for workplace surveillance to oversee the operation of workplace surveillance laws and to investigate and resolve complaints.[136] Rachel Dixon, Privacy and Data Protection Deputy Commissioner at OVIC, gave an example to illustrate this need:

> [M]ost state contracts, for example, contain clauses that say that contractors will delete the information, and under the IPPs they have to delete it when it is no longer required. If the employee has left, you do not really need to hold biometric information on them. But there is a cost to an employer of having somebody go into the system and delete all the biometrics that are associated with those people, so a lot of businesses do not do it, but you only find that out when the breach happens.
>
> … So unless you actually have some regulator who is going to do some random audits of things like that, you are never going to know. It is all great to have a piece of legislation that says everybody will delete these biometrics after, but you have to resource that or it is not going to be effective.[137]

Having an independent regulator not only gives workers an avenue to address grievances relating to workplace surveillance but also reinforces employer accountability.[138]

ACT workplace surveillance law provides for a regulator to administer the Workplace Privacy Act, inspect workplaces, investigate and resolve complaints and prosecute offences. Workplace inspectors under the *Work Health and Safety Act 2011* (ACT) have the power to inspect a workplace and enforce compliance with workplace surveillance legislation.[139] In NSW, there is no specific regulator for its workplace surveillance law. Despite the NSW Privacy Commissioner receiving a number of complaints about workplace surveillance, there have been no successful prosecutions, and the Commissioner has called for a regulator with powers to inspect workplaces, investigate complaints and prosecute offences to be appointed.[140]

In its recent Inquiry into the digital transformation of workplaces, the Australian House of Representatives Standing Committee on Employment, Education and Training recommended the Australian Government empower the Fair Work Commission to manage the dispute resolution process for complaints around breaches to workers' privacy, since 'the Privacy Act is not well equipped to deal with such workplace

---

136 National Tertiary Education Union, *Submission 24*, p. 25; Australian Nursing and Midwifery Federation, *Submission 38*, p. 13; Australian Services Union, Victorian Private Sector Branch, *Submission 41*, p. 5; Chris Molnar, *Transcript of evidence*, p. 28; Dr Jean Linis-Dinco, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 24; Associate Professor Alysia Blackham, *Transcript of evidence*, p. 44.

137 Rachel Dixon, *Transcript of evidence*, p. 15.

138 Dr Jean Linis-Dinco, *Transcript of evidence*, p. 24.

139 *Workplace Privacy Act 2011* (ACT) ss 43A, 43B, 43C; Brown and Witzleb, 'Big brother at work', p. 25; Dr Jacqueline Meredith, *Transcript of evidence*, p. 7.

140 Brown and Witzleb, 'Big brother at work', p. 25; Murray Brown, Barrister and Solicitor, public hearing, Melbourne, 26 September 2024, *Transcript of evidence*, p. 43.

disputes.'[141] While this may be one solution for Victoria, it is not clear at the time of this current report's tabling if the Australian Government supports the implementation of this recommendation. The importance of holding employers accountable and creating a mechanism for workers to make a complaint warrants Victoria appointing its own regulator to oversee the state's workplace surveillance legislation.

Appointing an existing body to regulate workplace surveillance in Victoria was preferred by many stakeholders in this current Inquiry and the Committee heard of several potential options, namely, OVIC, WorkSafe Victoria and Wage Inspectorate Victoria, which regulates certain state employment laws such as wage theft and long service leave. The choice would depend on how Victoria's workplace surveillance laws are framed. If the new laws take an industrial relations approach where employers and employees would negotiate to reach an agreement on workplace surveillance activities, then WorkSafe and the Wage Inspectorate might be best placed to regulate. If the laws are framed around privacy rules or principles, then OVIC would be the most appropriate regulator.[142]

OVIC supported itself being assigned to regulate workplace surveillance because:

- it already has expertise in this area with VPS organisations
- having a single regulator for privacy laws would make it easier for Victorians to navigate
- it is well placed to provide and develop educational resources
- it can leverage its relationship with OAIC to ensure consistency and coordination with the APPs.[143]

Law academics agreed that OVIC's experience with overseeing privacy and data protection made it an appropriate choice.[144]

WorkSafe Victoria was also proposed because of its experience with inspecting workplaces, mediating disputes between employers and employees, and overseeing consultation and negotiation in the occupational health and safety area.[145] However, WorkSafe Victoria's Chief Executive Officer Joe Calafiore felt that workplace surveillance did not clearly fit within WorkSafe's legislative remit, and the choice of regulator was a policy matter for government.[146] Wage Inspectorate Victoria was

---

141 Parliament of Australia, House of Representatives Standing Committee on Employment, Education and Training, *The future of work*, pp. 56, 58.

142 Office of the Victorian Information Commissioner, *Submission 39A*, p. 5; Matt O'Connor, Deputy Secretary, Industrial Relations Victoria, Department of Treasury and Finance, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 5.

143 Office of the Victorian Information Commissioner, *Submission 39A*, pp. 5–6; Sean Morrison, *Transcript of evidence*, p. 14.

144 Associate Professor Normann Witzleb, *Transcript of evidence*, p. 43; Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 45.

145 Laura Boehm, Industrial Officer, Australian Services Union, Victorian Private Sector Branch, public hearing, Melbourne, 3 September 2024, *Transcript of evidence*, p. 40; Dr Jacqueline Meredith, *Transcript of evidence*, p. 7; Chris Molnar, *Transcript of evidence*, p. 28.

146 Joe Calafiore, Chief Executive Officer, WorkSafe Victoria, public hearing, Melbourne, 1 November 2024, *Transcript of evidence*, p. 26.

suggested due to its powers to enforce and prosecute breaches of certain workplace laws.[147]

Another option would be having two regulators where OVIC would be responsible for the privacy aspect of workplace surveillance and WorkSafe or the Wage Inspectorate responsible for the industrial relations aspect.[148] However, having two regulators is likely to create confusion for employers and employees, especially if there is overlap and possibly different standards or applications between regulators.[149] A similar situation exists currently in Victoria where OVIC regulates the IPPs and the Health Complaints Commissioner regulates the Health Privacy Principles that cover health information. This has created administrative inefficiencies for both organisations, as well as for individuals who wish to make a complaint. Having a single regulator for workplace surveillance would be a more efficient option that would assist with compliance and public awareness.[150]

The Committee heard that whichever body is appointed to regulate workplace surveillance in Victoria, it must be adequately funded and resourced to perform that function properly.[151] Adequate resourcing is necessary due to increasing access to surveillance technology and the growing popularity of surveillance among employers.[152]

FINDING 29: An independent regulator of workplace surveillance would keep employers accountable and give employees an avenue to address any grievances.

RECOMMENDATION 18: That the Victorian Government appoint the Office of the Victorian Information Commissioner, WorkSafe Victoria or other appropriate body as a regulator and adequately resource it to oversee new workplace surveillance legislation with the power to inspect workplaces, investigate and resolve complaints, and prosecute offences.

147 Chris Molnar, *Transcript of evidence*, p. 28.

148 Office of the Victorian Information Commissioner, *Submission 39A*, p. 6.

149 Ibid.; Associate Professor Normann Witzleb, *Transcript of evidence*, p. 44; Rachel Dixon, *Transcript of evidence*, p. 15.

150 Office of the Victorian Information Commissioner, *Submission 39A*, p. 6; Associate Professor Normann Witzleb, *Transcript of evidence*, p. 43.

151 Sean Morrison, *Transcript of evidence*, p. 14; Adjunct Professor Moira Paterson, *Transcript of evidence*, p. 45; Associate Professor Alysia Blackham, *Transcript of evidence*, p. 44.

152 Office of the Victorian Information Commissioner, *Submission 39A*, p. 6.

Chapter 6
Conclusion

Workers' privacy is under threat from the growing use of surveillance devices in the workplace. Monitoring employees is not new, but surveillance technology is becoming more accessible, cheaper and easier to use, and employers are increasingly embracing surveillance, particularly after the shift to remote working as a result of the COVID-19 pandemic lockdowns.

Throughout this Inquiry, the Committee heard how many Victorian employees are unaware of the extent, methods and uses of surveillance in their workplace and unions are finding out these details at disciplinary meetings, following dismissals or by chance when employers or industry groups mention the types of technologies they use in the workplace. Workers and unions are also concerned about employers using artificial intelligence to process workplace surveillance data that is then used to measure performance or reach employment decisions in an opaque and potentially unfair way.

Studies have shown that intrusive workplace surveillance that lacks transparency reduces employees' job satisfaction, trust in management and commitment to their organisation. It appears to have minimal impact on productivity and may lead to counterproductive behaviours instead. Furthermore, excessive workplace surveillance has been shown to intensify work, adversely affect workers' mental and physical health, and exacerbate the power imbalance between employers and employees.

As this report has proven, state and federal laws have not kept pace with developments in workplace surveillance. The *Surveillance Devices Act 1999* (Vic) is ineffective because it is limited to prohibiting surveillance in workplace toilets, change rooms, washrooms and lactation rooms, and its definitions of tracking devices and private conversations and activities mean that few instances of workplace surveillance fall within the scope of the Act. Data surveillance is not even addressed, except for its use by law enforcement officers.

Federal laws do not address workplace surveillance. The *Fair Work Act 2009* (Cth) expressly leaves workplace surveillance to be regulated by the states and territories, and the *Privacy Act 1988* (Cth), which is concerned with protecting the privacy of individuals' personal information, contains exemptions for employee records and small businesses, leaving a significant gap in terms of workers' privacy and data protection.

New South Wales and the Australian Capital Territory (ACT) have dedicated workplace surveillance laws that require employers to provide employees with advance notice of workplace surveillance that specifies how and when it will be conducted. The ACT law goes even further, requiring employers to specify the purpose of the surveillance, consult with workers about its introduction or any changes, and give workers access to their data. It also requires employers to retain surveillance data for no longer than necessary and protect it from misuse, loss or unauthorised access, modification and disclosure.

The Committee recommends that Victoria introduce a new principles-based workplace surveillance law that ensures any workplace surveillance is reasonable, necessary and proportionate to achieve an employer's legitimate objective. Basing workplace surveillance legislation on these principles is technology neutral, making it adaptable to future advances. It also enables employers to continue using surveillance but in a way that recognises and protects workers' rights.

The Committee also recommends that employers be required to notify workers of proposed surveillance and specify the methods, scope, timing and purpose of the surveillance and how the data will be used and stored. In addition, employers should be required to consult with their employees about proposed surveillance and ensure a human has reviewed any automated decision made using workplace surveillance data that could significantly affect a worker's rights or interests.

The Inquiry also considered the protection of workplace surveillance data, which is insufficiently regulated by current state and federal privacy laws. The European Union's General Data Protection Regulation is considered best practice for protecting the privacy of individuals' data and its key principles have guided the Committee's recommendations to ensure workplace surveillance data is only collected for specified legitimate purposes, stored securely and kept for no longer than necessary. The Committee also recommends strengthening protections around biometric data, introducing a mandatory data breach notification scheme, extending privacy protections to all Victorian employees and appointing an independent regulator.

Workplace surveillance has legitimate purposes such as protecting property and workers' health and safety. However, current surveillance technologies make it easy for employers to use it for reasons that go beyond what is needed to fulfil business functions and keep people and property safe. The implementation of this report's recommendations will balance employers' interests with protecting employees' rights and privacy.

Adopted by the Legislative Assembly Economy and Infrastructure Committee
Parliament of Victoria, East Melbourne
31 March 2025

Appendix A
About the Inquiry

A.1 Submissions

Submission number	Individual or organisation	Date received
1	Robert Heron	4 June 2024
2	Kenneth McLeod	11 June 2024
3	Paul Murray	11 June 2024
4	Name withheld	17 June 2024
5	Business Council of Australia	11 July 2024
6	Dr Jean Linis-Dinco	11 July 2024
7	Australian Lawyers Alliance	15 July 2024
8	Professor Peter Leonard, Principal, Data Synergies and Professor of Practice, UNSW Business School	16 July 2024
9	Aijaz Moinuddin	17 July 2024
10	Australian HR Institute	18 July 2024
11	Master Electricians Australia	18 July 2024
12	Laundry Association Australia	18 July 2024
13	Centre for Decent Work and Industry, QUT	19 July 2024
14	Institute of Mercantile Agents	19 July 2024
15	Ramsay Health Care Australia	19 July 2024
16	Victorian Farmers Federation	19 July 2024
17	Construction, Forestry and Maritime Employees Union, Manufacturing Division	20 July 2024
18	Victorian Chamber of Commerce and Industry	22 July 2024
19	Communication Workers Union, Postal and Telecommunication Branch Victoria	22 July 2024
20	Community and Public Sector Union, Victorian Branch	29 July 2024
21	Australian Security Industry Association Limited	30 July 2024
22	Professor Peter Holland and Jacqueline Meredith, Swinburne University of Technology	30 July 2024
23	Independent Education Union, Victoria Tasmania Branch	30 July 2024
24	National Tertiary Education Union	30 July 2024
25	United Workers Union	30 July 2024
26	Victorian Automotive Chamber of Commerce	31 July 2024
27	Australian Workers' Union	31 July 2024

A

Submission number	Individual or organisation	Date received
28	Victorian Trades Hall Council	31 July 2024
29	Australian Services Union, Victorian and Tasmanian Authorities and Services Branch	31 July 2024
30	Name withheld	31 July 2024
31	Australian Manufacturing Workers' Union	31 July 2024
32	Centre for Future Work, Australia Institute	31 July 2024
33	Charles Mitchell	31 July 2024
34	Dr Dale Tweedie, Senior Lecturer, Department of Accounting and Corporate Governance, Macquarie University	31 July 2024
35	Finance Sector Union	31 July 2024
36	Building Industry Group of Unions	1 August 2024
37	Law Institute of Victoria	1 August 2024
38	Australian Nursing and Midwifery Federation, Victorian Branch	2 August 2024
39	Office of the Victorian Information Commissioner	2 August 2024
39A	Supplementary submission	2 October 2024
40	Australian Industry Group	4 August 2024
41	Australian Services Union, Victorian Private Sector Branch	7 August 2024
42	Australian Education Union, Victorian Branch	12 August 2024
43	Victorian Government	30 August 2024
44	Commonwealth Bank of Australia	18 October 2024

A.2 Public hearings

Tuesday 3 September 2024

Melbourne

Name	Title	Organisation
Professor Peter Holland	Professor, Human Resource Management, School of Business, Law and Entrepreneurship	Swinburne University of Technology
Dr Jacqueline Meredith	Lecturer, Swinburne Law School	Swinburne University of Technology
Sean Morrison	Victorian Information Commissioner	Office of the Victorian Information Commissioner
Rachel Dixon	Privacy and Data Protection Deputy Commissioner	Office of the Victorian Information Commissioner
Kat Eather	General Counsel	Business Council of Australia
Chris Molnar	Co-Chair, LIV Workplace Relations Committee	Law Institute of Victoria
Donna Cooper	General Manager, Policy, Advocacy and Professional Standards	Law Institute of Victoria

Name	Title	Organisation
Danae Bosler	Assistant Secretary-by-Appointment	Victorian Trades Hall Council
Wilhemina Stracke	Assistant Secretary	Victorian Trades Hall Council
Oscar Kaspi-Crutchett	Researcher	Victorian Trades Hall Council
Leroy Lazaro	Branch Secretary	Communication Workers Union, Postal and Telecommunication Branch Victoria
Troy McGuinness	Elected Organiser	Communication Workers Union, Postal and Telecommunication Branch Victoria
Karen Batt	Secretary	Community and Public Sector Union, Victorian Branch
Jason Cleeland	Manager, Membership and Information Technology	Community and Public Sector Union, Victorian Branch
Tash Wark	Secretary	Australian Services Union, Victorian and Tasmanian Authorities and Services Branch
Simon Hammersley	Research and Policy Adviser	Australian Services Union, Victorian and Tasmanian Authorities and Services Branch
Nicole McPherson	National Assistant Secretary	Finance Sector Union
Matthew Rowe	National Executive Member	Finance Sector Union
Laura Boehm	Industrial Officer	Australian Services Union, Victorian Private Sector Branch
Kat Hardy	Lead Organiser	Australian Services Union, Victorian Private Sector Branch
Jenny Kruschel	National Secretary, Textile Clothing Footwear	Construction, Forestry and Maritime Employees Union, Manufacturing Division
Paris Nicholls	Senior National Industrial Officer	Construction, Forestry and Maritime Employees Union, Manufacturing Division
Stephen Fodrocy	Industrial Officer	Australian Manufacturing Workers' Union
Luke Souvatzis	Union Official	Australian Manufacturing Workers' Union

Monday 23 September 2024

Melbourne

Name	Title	Organisation
Professor John Howe		Centre for Employment and Labour Relations Law, Melbourne Law School, University of Melbourne
Professor Peter Leonard	Principal Professor of Practice	Data Synergies UNSW Business School
Chris Delaney	Industrial Relations Advisor	Australian Security Industry Association Limited

A

Name	Title	Organisation
Peter Johnson	Compliance and Regulatory Affairs Advisor	Australian Security Industry Association Limited
Luke Simpkins	CEO	Laundry Association Australia
Michael Johns	CEO, Bundle Australia	Laundry Association Australia
Christopher Murphy	Director, Spindle Australia/ New Zealand	Laundry Association Australia
Alison Smith	Manager, People and Culture, SPL	Laundry Association Australia
Jody Wright	CEO	Institute of Mercantile Agents
Amy Elliot	Chairperson, Investigations Sector	Institute of Mercantile Agents
Associate Professor Penelope Williams	Director	Centre for Decent Work and Industry, QUT
Danae Fleetwood	Master of Philosophy research student	Centre for Decent Work and Industry, QUT
Susan Accary	President, Victoria Branch Committee	Australian Lawyers Alliance
Sha Hotchin	Secretary, Victoria Branch Committee	Australian Lawyers Alliance

Thursday 26 September 2024

Melbourne

Name	Title	Organisation
James Fleming	Executive Director	Australian Institute of Employment Rights
Sunil Kemppi	Vice President, Employee Representative	Australian Institute of Employment Rights
Dr Allan McCay	Academic Fellow	Sydney Law School, University of Sydney
	Co-Director	The Sydney Institute of Criminology
	President	Institute of Neurotechnology and Law
Dr Dale Tweedie	Senior Lecturer, Department of Accounting and Corporate Governance	Macquarie University
Dr Fiona Macdonald	Policy Director, Industrial and Social	Centre for Future Work, Australia Institute
Dr Jean Linis-Dinco		
Chris Lehmann	General Manager, Membership, Advocacy and Partners	Master Electricians Australia
Georgia Holmes	Policy and Communications Advisor	Master Electricians Australia
Daniel Hodges	Executive Manager, Workplace Relations	Victorian Automotive Chamber of Commerce
Scott Barklamb	Principal Advisor, Workplace Relations Policy	Australian Industry Group
Yoness Blackmore	Principal Advisor, Workplace Relations Policy	Australian Industry Group

Name	Title	Organisation
Associate Professor Normann Witzleb		Faculty of Law, Monash University and Faculty of Law, The Chinese University of Hong Kong
Murray Brown	Barrister and Solicitor	
Adjunct Professor Moira Paterson		Castan Centre for Human Rights Law, Faculty of Law, Monash University

Friday 1 November 2024

Melbourne

Name	Title	Organisation
Matt O'Connor	Deputy Secretary	Industrial Relations Victoria, Department of Treasury and Finance
Sharon De Silva	Director, Secure Work	Industrial Relations Victoria, Department of Treasury and Finance
Amelia Bitsis	Executive Director, Policy and Advocacy	Victorian Chamber of Commerce and Industry
Caitlin Hardy	Principal Adviser, Policy and Advocacy	Victorian Chamber of Commerce and Industry
Joe Calafiore	Chief Executive Officer	WorkSafe Victoria
Amy Salmon	Principal Psychological Health and Safety Specialist	WorkSafe Victoria
Emma Germano	President	Victorian Farmers Federation
Charles Everist	General Manager, Policy and Advocacy	Victorian Farmers Federation
David Brear	General Secretary	Independent Education Union, Victoria Tasmania Branch
Liam Hanlon	Industrial Officer	Independent Education Union, Victoria Tasmania Branch
Sarah Roberts	Secretary, Victorian Division	National Tertiary Education Union
Associate Professor Alysia Blackham		National Tertiary Education Union
Lauren Kelly	Research and Policy Officer	United Workers Union
Alana Ginnivan	Professional Officer	Australian Nursing and Midwifery Federation, Victorian Branch
Libby Muir	Professional Officer	Australian Nursing and Midwifery Federation, Victorian Branch
Dr Jake Goldenfein	Senior Lecturer and Chief Investigator of ADM+S Centre (University of Melbourne node)	ARC Centre of Excellence for Automated Decision-Making and Society, RMIT

Glossary

Algorithmic bias	Where an artificial intelligence (AI) system makes errors and produces unfair or discriminatory results. This might be due to the design of the model, but more likely the data used to train it.
Algorithmic decision-making	The use of AI to process data and make automated decisions utilising algorithms.
Artificial intelligence (AI)	Technology that can perform tasks such as generating content, forecasts and decisions independently of humans.
Biometric surveillance	The collection or recording of biological or physical characteristics to identify an individual. Biometric data can include fingerprints, iris scans and retinal scans, facial and voice recognition, swabs and blood samples.
Data surveillance	The monitoring of a person's actions or communications through digital means such as computer usage, email communications and internet activity using tools such as keystroke monitoring, cookies or spyware.
Function creep	Where surveillance that is implemented for one purpose gets used covertly for other purposes.
Information privacy	Protection of an individual's personal information. In terms of workplace surveillance, information privacy is an employee's ability to control who can see or use their personal information, how and when this information is collected and how it can be used.
Listening surveillance	The monitoring or recording of conversations through microphones or voice recorders or by intercepting phone calls or online voice communications.
Neurosurveillance	The use of neurotechnology to monitor a person's cognitive state such as their level of attention and effort.
Optical surveillance	The monitoring or recording of images of a person or place through visual aids, cameras, video recorders or closed-circuit television.
Personal information	A broad range of information, or an opinion, that could identify an individual, including names, contact details, photos, bank account details, tax file numbers, driver licence details and work records such as performance evaluations.
Psychosocial hazard	Any risk in the workplace that can cause stress and result in psychological or physical harm.
Sensitive personal information	A subset of personal information that includes information about a person's health, ethnicity, sexual orientation, political associations, religious beliefs, trade union memberships, criminal records and biometric data.
Surveillance	The purposeful monitoring of a person, place or object to obtain information and/or influence the behaviour of the person being monitored. It can be overt, if the person being monitored is aware that surveillance is happening or the surveillance device is not concealed, or covert, where the person is unaware of the monitoring or the device is concealed.
Tracking surveillance	The monitoring or recording of a person's or object's location or movements at a particular time using technologies such as Global Positioning System (GPS) tracking, radio frequency identification (RFID) and automatic number plate recognition.
Works councils	Bodies of employee representatives within a single workplace.

Bibliography

Attorney-General's Department, *Privacy Act review: report on a page*, factsheet, Australian Government, Canberra, February 2023.

Attorney-General's Department, *Privacy Act review: report*, Australian Government, Canberra, 2022.

Attorney-General's Department, *Reform of Australia's electronic surveillance framework*, 2020, <https://www.ag.gov.au/crime/telecommunications-interception-and-surveillance/reform-australias-electronic-surveillance-framework> accessed 22 November 2024.

Attorney-General's Department, *Commonwealth Government response to the comprehensive review of the legal framework of the national intelligence community*, Australian Government, Canberra, 2020.

Australian Bureau of Statistics, *Counts of Australian businesses, including entries and exits*, 2023, <https://www.abs.gov.au/statistics/economy/business-indicators/counts-australian-businesses-including-entries-and-exits/jul2019-jun2023> accessed 22 November 2024.

Australian Government, *Government response: Privacy Act review report*, Canberra, 2023.

Australian Human Rights Commission, *Protecting cognition: background paper on human rights and neurotechnology*, Sydney, 2024.

Australian Human Rights Commission, *Using artificial intelligence to make decisions: addressing the problem of algorithmic bias*, report prepared by Finn Lattimore, Simon O'Callaghan, Zoe Paleologos, Alistair Reid, Edward Santow, Holli Sargeant and Andrew Thomsen, Sydney, 2020.

Australian Institute of Employment Rights, *Ron McCallum debate: transcript*, supplementary evidence received 2 October 2024.

Australian Law Reform Commission, *Serious invasions of privacy in the digital era: final report*, Australian Government, Sydney, 2014.

Australian Law Reform Commission, *For your information: Australian privacy law and practice*, report 108, vol. 1, Australian Government, Sydney, 2008.

Australian Nursing and Midwifery Federation, Victorian Branch, *Hearing notes*, supplementary evidence received 1 November 2024.

Ball, Kirstie, *Electronic monitoring and surveillance in the workplace: literature review and policy recommendations*, Publications Office of the European Union, Luxembourg, 2021.

Blackham, Alysia, 'Surveillance, data collection and privacy at work: a new application of equitable obligations?', *Australian Journal of Labour Law*, (forthcoming), 2025, pp. 1–25.

Blackham, Alysia, 'Setting the framework for accountability for algorithmic discrimination at work', *Melbourne University Law Review*, vol. 47, no. 63, 2023, pp. 63–113.

Bogle, Ariel, ''Stop all time wasting': Woolworths workers tracked and timed under new efficiency crackdown', *The Guardian*, 23 October 2024, <https://www.theguardian.com/business/2024/oct/23/woolworths-staff-efficiency-productivity-crackdown-timed> accessed 25 October 2024.

Bronowicka, Joanna, Mirela Ivanova, Wojciech Klicki, Seán King, Eva Kocher, Julia Kubisa and Justyna Zielińska, *'Game that you can't win'?: workplace surveillance in Germany and Poland*, European University Viadrina, Frankfurt, 2020.

Brown, Murray and Chris Dent, 'Privacy concerns over employer access to employee social media', *Monash University Law Review*, vol. 43, no. 3, 2017, pp. 796–827.

Brown, Murray and Normann Witzleb, 'Big brother at work: workplace surveillance and employee privacy in Australia', *Australian Journal of Labour Law*, vol. 34, no. 3, 2021, pp. 170–199.

Brownell, Claire, 'The boss is watching', *Maclean's*, 15 December 2020, <https://macleans.ca/society/the-workplace-of-the-future-will-probably-remain-under-surveillance> accessed 12 June 2024.

Chen, Colleen and John Howe, *Worker data right: the digital right of entry*, policy brief, no. 5, Centre for Employment and Labour Relations Law, University of Melbourne, 2022.

Clarke, Roger, 'Responsible application of artificial intelligence to surveillance: what prospects?', *Information Polity*, vol. 27, no. 2, 2022, pp. 175–191.

Collins, Benedict, 'Best employee monitoring software of 2024', *TechRadar*, 4 July 2024, <https://www.techradar.com/best/best-employee-monitoring-software> accessed 17 July 2024.

Cutter, Chip and Te-Ping Chen, 'Bosses aren't just tracking when you show up to the office but how long you stay', *The Wall Street Journal Online*, 26 September 2023, <https://www.wsj.com/lifestyle/careers/attention-office-resisters-the-boss-is-counting-badge-swipes-5fa37ff7> accessed 12 June 2024.

Dawson, Sophie, Emily Lau and Lydia Cowan-Dillon, 'Practical implications of the new transparency requirements for automated decision making', *Johnson Winter*

Slattery, 14 January 2025, <https://jws.com.au/what-we-think/practical-implications-of-new-transparency-requirements-for-automated-decision-making> accessed 20 January 2025.

de Flamingh, Jack and Phillip Magness, 'The limitations of a modern day bag search', *Law Society Journal*, no. 48, September 2018, pp. 76–77.

De Hert, Paul and Georgios Bouchagiar, 'Visual and biometric surveillance in the EU. Saying 'no' to mass surveillance practices?', *Information Polity*, vol. 27, no. 2, 2022, pp. 193–217.

Department of Education, Victoria, *Photographing, filming and recording staff and other adults*, 2020, <https://www2.education.vic.gov.au/pal/photographing-staff/policy> accessed 6 February 2025.

Department of Industry, Science and Resources, National Artificial Intelligence Centre, *Voluntary AI safety standard*, Australian Government, August 2024.

Department of Justice and Attorney-General, *Civil surveillance reforms*, Queensland Government, Brisbane, 2023.

Eurofound, *Employee monitoring and surveillance: the challenges of digitalisation*, Publications Office of the European Union, Luxembourg, 2020.

European Union, *Directive of the European Parliament and of the Council on improving working conditions in platform work*, Brussels, 2024.

European Union, *General Data Protection Regulation*, 2018, <https://gdpr-info.eu> accessed 3 February 2025.

Fair Work Ombudsman, *Workplace privacy best practice guide*, Australian Government, 2023.

Future of Privacy Forum, *Best practices for AI and workplace assessment technologies*, Washington, 2023.

Government of New South Wales, *Response to the Parliament of New South Wales, Legislative Council Select Committee on the impact of technological and other change on the future of work and workers in New South Wales, report no. 2—workplace surveillance and automation*, 2023.

Griffiths, Owen and David McGovern, *Privacy and Other Legislation Amendment Bill 2024*, bills digest, no. 16, 2024–25, Parliament of Australia Library, November 2024.

Heap, Lisa, *No blood—no job: Australia's privacy laws and workers' rights*, Centre for Future Work, Australia Institute, 2024.

Henderson, Troy, Tom Swann and Jim Stanford, *Under the employer's eye: electronic monitoring & surveillance in Australian workplaces*, Centre for Future Work, Australia Institute, 2018.

Holland, Peter and Tse Leng Tham, 'Workplace biometrics: protecting employee privacy one fingerprint at a time', *Economic and Industrial Democracy*, vol. 43, no. 2, 2022, pp. 501–551.

Information Commissioner's Office UK, *Employment practices and data protection: monitoring workers*, October 2023, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers> accessed 14 May 2024.

Information Commissioner's Office UK, *Overview—data protection and the EU*, (n.d.), <https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu> accessed 3 February 2025.

Institute for Public Policy Research, *Watching me, watching you: worker surveillance in the UK after the pandemic*, report prepared by Henry Parkes, London, 2023.

International Labour Organization, *Protection of Workers' Personal Data: an ILO code of practice*, International Labour Office, Geneva, 1997.

Jeske, Debora, 'Remote workers' experiences with electronic monitoring during Covid-19: implications and recommendations', *International Journal of Workplace Health Management*, vol. 15, no. 3, 2022, pp. 393–409.

Kalischko, Thomas and René Riedl, 'Electronic performance monitoring in the digital workplace: conceptualization, review of effects and moderators, and future research opportunities', *Frontiers in Psychology*, vol. 12, 2021, pp. 1–15, doi: 10.3389/fpsyg.2021.633031

Kayas, Oliver G., 'Workplace surveillance: a systematic review, integrative framework, and research agenda', *Journal of Business Research*, vol. 168, 2023, pp. 1–16, doi: 10.1016/j.busres.2023.114212

Lazar, Wendi S. and Cody Yorke, 'Watched while working: use of monitoring and AI in the workplace increases', *Reuters*, 26 April 2023, <https://www.reuters.com/legal/legalindustry/watched-while-working-use-monitoring-ai-workplace-increases-2023-04-25> accessed 16 May 2024.

Leonard, Peter, 'Workplace surveillance and privacy', *Computers and Law: Journal for the Australian and New Zealand Societies for Computers and the Law*, vol. 93, 2021, pp. 60–73.

Maati, Ahmed, 'Long-term prescription?: digital surveillance is here to stay', *Czech Journal of International Relations*, vol. 56, no. 4, 2021, pp. 105–118.

Macdonald, Dr Fiona and Dr Lisa Heap, Centre for Future Work, Australia Institute, *Inquiry into the digital transformation of workplaces*, submission to House of Representatives Standing Committee on Employment, Education and Training, 2024.

Magner, Aaron and Steven Penning, 'Workplace surveillance and privacy', *Commercial Law Quarterly*, vol. 20, September–November, 2006, pp. 24–33.

McDonald, Peter, 'Robodebt is just one reason why we should be worried about AI', *Centre for Social Impact*, 14 August 2023, <https://www.csi.edu.au/news/robodebt-is-just-one-reason-why-we-should-be-worried-about-ai> accessed 13 December 2024.

McGrath, Geoff, Leon Franklin, Robert Todd, Clare Doneley and Andrew Hilton, *Australia's first tranche of privacy reforms: a deep dive and why they matter*, Ashurst, 2024, <https://www.ashurst.com/en/insights/australias-first-tranche-of-privacy-reforms-a-deep-dive-and-why-they-matter> accessed 23 January 2025.

Morgan, Kate and Delaney Nolan, 'How worker surveillance is backfiring on employers', *BBC*, 30 January 2023, <https://www.bbc.com/worklife/article/20230127-how-worker-surveillance-is-backfiring-on-employers> accessed 15 May 2024.

Nahum, Dan, *Working from home, or living at work?: hours of work, unpaid overtime, and working arrangements through COVID-19*, Centre for Future Work, Australia Institute, 2021.

Nahum, Dan and Jim Stanford, Centre for Future Work, Australia Institute, *Technology, standards and democracy*, submission to NSW Legislative Council Select Committee on the Impact of technological and other change on the future of work and workers in New South Wales, 2020.

Negrón, Wilneida and Aiha Nguyen, 'The long shadow of workplace surveillance', *Stanford Social Innovation Review*, 6 September 2023, <https://ssir.org/articles/entry/the_long_shadow_of_workplace_surveillance> accessed 17 July 2024.

Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, Australian Government, Sydney, 2022.

Office of the Australian Information Commissioner, *Employment*, (n.d.), <https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/employment> accessed 22 November 2024.

Office of the Victorian Information Commissioner, *Guiding principles for surveillance*, 2022, <https://ovic.vic.gov.au/privacy/resources-for-organisations/guiding-principles-for-surveillance> accessed 13 May 2024.

Office of the Victorian Information Commissioner, *Information privacy principles: full text*, 2021, <https://ovic.vic.gov.au/privacy/resources-for-organisations/information-privacy-principles-full-text/> accessed 22 November 2024.

Office of the Victorian Information Commissioner, *EU general data protection regulation*, 2020, <https://ovic.vic.gov.au/privacy/resources-for-organisations/eu-general-data-protection-regulation> accessed 16 May 2024.

Office of the Victorian Information Commissioner, *Your privacy rights*, 2020, <https://ovic.vic.gov.au/privacy/for-the-public/your-privacy-rights> accessed 22 November 2024.

Office of the Victorian Information Commissioner, *Privacy during employment*, 2019, <https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-during-employment> accessed 10 May 2024.

Parliament of Australia, House of Representatives Standing Committee on Employment, Education and Training, *The future of work: Inquiry into the digital transformation of workplaces*, February 2025.

Parliament of Australia, House of Representatives Standing Committee on Employment, Education and Training, *Terms of reference, Inquiry into the digital transformation of workplaces*, 9 April 2024, <https://www.aph.gov.au/Parliamentary_Business/Committees/House/Employment_Education_and_Training/DigitalTransformation/Terms_of_Reference> accessed 22 November 2024.

Parliament of New South Wales, Legislative Council Select Committee on the Impact of Technological and Other Change on the Future of Work and Workers in New South Wales, *Impact of technological and other change on the future of work and workers in New South Wales: final report—workplace surveillance and automation*, November 2022.

Ravid, Daniel M., Jerod C. White, David L. Tomczak, Ahleah F. Miles and Tara S. Behrend, 'A meta-analysis of the effects of electronic performance monitoring on work outcomes', *Personnel Psychology*, vol. 76, no. 5, 2023, pp. 5–40.

Rogers, Brishen, 'The law and political economy of workplace technological change', *Harvard Civil Rights—Civil Liberties Law Review*, vol. 55, 2020, pp. 531–584.

Siegel, Rudolf, Cornelius J. König and Veronika Lazar, 'The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behavior: a meta-analysis', *Computers in Human Behavior Reports*, vol. 8, 2022, pp. 1–13, doi: 10.1016/j.chbr.2022.100227

Stanford, Jim, Director, Centre for Future Work, Australia Institute, *The future of work is what we make it*, submission to Senate Select Committee on the Future of Work and Workers, 2018.

State of California Department of Justice, *California Consumer Privacy Act (CCPA)*, 2024, <https://oag.ca.gov/privacy/ccpa> accessed 20 May 2024.

Stratton, Jim, 'The future of work starts with trust: how can we close the AI trust gap?', *World Economic Forum*, 15 January 2024, <https://www.weforum.org/agenda/2024/01/why-there-is-an-ai-trust-gap-in-the-workplace> accessed 17 July 2024.

Stryker, Cole and Eda Kavlakoglu, 'What is artificial intelligence (AI)?', *IBM*, 9 August 2024, <https://www.ibm.com/think/topics/artificial-intelligence> accessed 13 December 2024.

Tasmania Law Reform Institute, *Review of privacy laws in Tasmania*, final report, no. 33, Hobart, May 2024.

Teebken, Mena Angela and Thomas Hess, 'Privacy in a digitised workplace: towards an understanding of employee privacy concerns', *Proceedings of the 54th Hawaii International Conference on System Sciences*, 2021, pp. 6661–6670.

Thompson, Danielle E. and Adam Molnar, 'Workplace surveillance in Canada: a survey on the adoption and use of employee monitoring applications', *Canadian Review of Sociology*, vol. 60, 2023, pp. 801–819.

UK Government, *Factsheet: Employment Rights Bill overview*, (n.d.), <https://assets.publishing.service.gov.uk/media/6752f32a14973821ce2a6cc2/employment-rights-bill-overview.pdf> accessed 14 January 2025.

UK Parliament, *Inquiry launched into human rights at work*, 2023, <https://committees.parliament.uk/committee/93/human-rights-joint-committee/news/186147/inquiry-launched-into-human-rights-at-work> accessed 17 May 2024.

United Nations, *International Bill of Human Rights*, <https://www.ohchr.org/en/what-are-human-rights/international-bill-human-rights> accessed 17 December 2024.

United Nations, *International Covenant on Civil and Political Rights*, 1966, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> accessed 15 January 2025.

United Nations, *International Covenant on Economic, Social and Cultural Rights*, 1966, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights> accessed 15 January 2025.

United Nations, *Universal Declaration of Human Rights*, 1948, <https://www.un.org/en/about-us/universal-declaration-of-human-rights> accessed 15 January 2025.

Victorian Law Reform Commission, *Workplace privacy: final report*, Melbourne, 2005.

Victorian Trades Hall Council, *VTHC submission to the Inquiry into the digital transformation of workplaces*, submission to House of Representatives Standing Committee on Employment, Education and Training, 2024.

Wilson, John and Kieran Pender, 'The rights and wrongs of workplace surveillance', *Ethos: Law Society of the ACT Journal*, no. 267, 2023, pp. 24–28.

Extracts of proceedings

Legislative Assembly Standing Order 220(4) requires the Committee to include in its report to the House any division relating to the adoption of the draft report.

The Committee divided on the following questions during consideration of this report.

Committee meeting—31 March 2025

Anthony Cianflone moved that chapter 1 stand part of the report.

The Committee divided on the question.

Ayes 3	Noes 2
Alison Marchant	Kim O'Keeffe
Anthony Cianflone	Roma Britnell
John Mullahy	

Motion carried.

John Mullahy moved that chapter 2 stand part of the report.

The Committee divided on the question.

Ayes 3	Noes 2
Alison Marchant	Kim O'Keeffe
Anthony Cianflone	Roma Britnell
John Mullahy	

Motion carried.

Anthony Cianflone moved that chapter 3 stand part of the report.

The Committee divided on the question.

Ayes 3	Noes 2
Alison Marchant	Kim O'Keeffe
Anthony Cianflone	Roma Britnell
John Mullahy	

Motion carried.

John Mullahy moved that chapter 4 stand part of the report.

The Committee divided on the question.

Ayes 3	Noes 2
Alison Marchant	Kim O'Keeffe
Anthony Cianflone	Roma Britnell
John Mullahy	

Motion carried.

Anthony Cianflone moved that chapter 5 stand part of the report.

The Committee divided on the question.

Ayes 3	Noes 2
Alison Marchant	Kim O'Keeffe
Anthony Cianflone	Roma Britnell
John Mullahy	

Motion carried.

John Mullahy moved that chapter 6 stand part of the report.

The Committee divided on the question.

Ayes 3	Noes 2
Alison Marchant	Kim O'Keeffe
Anthony Cianflone	Roma Britnell
John Mullahy	

Motion carried.

Anthony Cianflone moved that the executive summary stand part of the report.

The Committee divided on the question.

Ayes 3	Noes 2
Alison Marchant	Kim O'Keeffe
Anthony Cianflone	Roma Britnell
John Mullahy	

Motion carried.

John Mullahy moved that the preliminary pages and appendices stand part of the report.

The Committee divided on the question.

Ayes 3	Noes 2
Alison Marchant	Kim O'Keeffe
Anthony Cianflone	Roma Britnell
John Mullahy	

Motion carried.

Anthony Cianflone moved that the bibliography stand part of the report.

The Committee divided on the question.

Ayes 3	Noes 2
Alison Marchant	Kim O'Keeffe
Anthony Cianflone	Roma Britnell
John Mullahy	

Motion carried.

John Mullahy moved that the draft final report (including chapters 1–6, executive summary, preliminary pages, appendices and bibliography), together with the correction of any typographical errors, be the final report of the Committee.

The Committee divided on the question.

Ayes 3	Noes 2
Alison Marchant	Kim O'Keeffe
Anthony Cianflone	Roma Britnell
John Mullahy	

Motion carried.

Minority report

INQUIRY INTO WORKPLACE SURVEILLANCE: MINORITY REPORT

LIBERAL AND NATIONALS

APRIL 2025

Kim O'Keeffe

The Nationals

Roma Britnell

Liberal Party

Nicole Werner

Liberal Party

Foreword by the Liberal and Nationals

This report by the Liberal and National Party members of the Legislative Assembly Economy and Infrastructure Committee Inquiry into Workplace Surveillance, respectfully dissent from the majority report and associated recommendations on workplace surveillance reform.

While we support the underlying intention to ensure fairness and respect for individual privacy, we strongly oppose the proposed regulatory approach.

We believe the majority report fails to adequately address stakeholder concerns, overreaches in its scope, and risks creating an unnecessary and inconsistent legal burden on employers, especially small businesses.

The Commonwealth Government is currently reviewing the Privacy Act 1998 (Cth) and it is our view that any legislative changes made purely in Victoria risk creating a fragmented approach to workplace surveillance and the potential for any changes to become null and void once reform is conducted at a Commonwealth level.

Recommendations

1. **That the Victorian Government defers any legislative action on workplace surveillance until the Commonwealth Government has completed a review of the Privacy Act 1998 (Cth).**

2. **That the Victorian Government in consultation with employer industry groups, develop best practice guidelines for employers undertaking workplace surveillance.**

3. **That the Victorian Government develops a clear definition of workplace surveillance that includes reference to work conducted away from a business' physical premises.**

4. **That any guidelines, policies, or legislation related to workplace surveillance specific to Victoria, consider and address the unique challenges faced by small businesses.**

5. **That any guidelines, policies, or legislation related to workplace surveillance specific to Victoria addresses the administrative burden of processing data requests, particularly for smaller employers.**

Commonwealth Regulation

The recommendations in the report risk fragmenting the national regulatory landscape by introducing state-specific laws while significant federal privacy reforms are still underway.

In its submission, the Business Council of Australia explicitly recommended that legislative reform be postponed until after the Commonwealth Government finalises its reforms to the Privacy Act 1998 (Cth), particularly in relation to the employee records exemption and the small business exemption.[1]

Pushing ahead unilaterally could lead to conflicting interpretations of key concepts, such as what constitutes a "workplace" or "reasonable surveillance", and may burden employers with overlapping obligations under state and federal law.

RECOMMENDATION ONE: That the Victorian Government defers any legislative action on workplace surveillance until the Commonwealth Government has completed a review of the Privacy Act 1998 (Cth).

Establishing Guidelines

Multiple employer groups, including the Business Council of Australia, Australian Industry Group, and the Victorian Chamber of Commerce and Industry, recommended a non-legislative approach to workplace surveillance reform.[2]

These submissions advocated for the development of best-practice guidelines or model policies rather than new statutory obligations.

These stakeholders argued that flexible, industry-informed guidance would provide more practical and less disruptive solutions to privacy concerns than the rigid, one-size-fits-all framework proposed in the report.

The Business Council of Australia specifically stated that "best practice guidelines, co-designed with employers, unions and relevant government agencies, would be more effective and less burdensome than broad new laws."[3]

RECOMMENDATION TWO: That the Victorian Government in consultation with employer industry groups, develop best practice guidelines for employers undertaking workplace surveillance.

Defining Workplace Surveillance

Several submissions during the Committee's Inquiry raised concerns about the lack of a clear, workable definition of "workplace surveillance", particularly as it related to hybrid and remote work environments.

[1] Business Council of Australia submission no.5, page 1.
[2] Australian Industry Group submission no.40, page 4.
[3] Business Council of Australia submission no.5, page 1.

The majority report proposes that the definition of workplace includes “wherever work occurs”, which could include private homes.

This approach risks enabling government overreach into private residences and fails to adequately consider the unique privacy concerns associated with home-based work.

RECOMMENDATION THREE: That the Victorian Government develops a clear definition of workplace surveillance that includes reference to work conducted away from a business’ physical premises.

Impact on Small Businesses

The Committee’s majority report fails to account the disproportionate impact these reforms would have on small and medium-sized businesses.

Stakeholders including the Victorian Chamber of Commerce and Industry, and Master Electricians Australia highlighted how requirements such as mandatory consultation, 14-day notice provisions, and written surveillance policies would be difficult for small businesses to implement.

These businesses often operate without in-house HR or legal teams, making compliance with complex new obligations particularly onerous.

As the Victorian Chamber of Commerce and Industry put it, “adding prescriptive workplace surveillance obligations will result in unnecessary compliance burdens for small enterprises.”[4]

RECOMMENDATION FOUR: That any guidelines, policies, or legislation related to workplace surveillance specific to Victoria, consider and address the unique challenges faced by small businesses.

Administrative Burdens

While well-intentioned, the proposal to grant employees access to surveillance data (e.g. CCTV footage, keyboard tracking logs) could infringe the privacy of other individuals.

WorkSafe Victoria, in its evidence to the Committee, cautioned that this measure could compromise the privacy of co-workers, or third parties inadvertently captured in surveillance data.[5]

This recommendation also fails to address the administrative burden of processing such requests, particularly for smaller employers.

[4] Victorian Chamber of Commerce and Industry, public hearing, 1 November 2024. *Transcript of evidence*, page 14.
[5] WorkSafe Victoria, public hearing, 1 November 2024. *Transcript of evidence*, pages 24 and 26.

RECOMMENDATION FIVE: That any guidelines, policies, or legislation related to workplace surveillance specific to Victoria addresses the administrative burden of processing data requests, particularly for smaller employers.

Other Areas of Concern

Potential for union overreach and weaponisation

The majority report does not address the potential for mandatory consultation, disclosure obligations, and data access rights to be misused in industrial disputes.

These mechanisms could be weaponised by unions or others to exert pressure on employers, delay enterprise bargaining processes, or generate frivolous complaints.

Examples of misuse could include:

- Flooding small businesses with access or consultation requests.
- Using surveillance records to mount strategic or vexatious grievances.
- Disrupting business operations under the pretext of enforcing new rights.

The majority report's failure to consider this risk is a critical oversight that undermines the credibility of its recommendations.

Lack of evidence of widespread abuse

The majority report also does not provide compelling evidence that workplace surveillance is currently being abused at scale in Victoria.

No systemic issues were identified that would warrant such sweeping legislative intervention. Regulation must be proportionate to the demonstrated harm, and in this case, the problem has not been sufficiently established.

Conclusion

The Liberal and National Party members of the Committee believe the majority report oversteps what is necessary, reasonable, and practical.

Rather than introducing complex new laws, we urge the Victorian Government to consult further with employer groups, prioritise national consistency, and adopt a more balanced, education-led approach that recognises the legitimate interests of both employers and employees.

Until a clear case is made, and national reforms are finalised, we cannot support the recommendations in their current form.