Ai GROUP SUBMISSION

Victorian Legislative Assembly
Economy & Infrastructure Committee

Inquiry into Workplace Surveillance

4 AUGUST 2024

CONTENTS

	Section	Page
1	Inquiry Into Workplace Surveillance	3
	PART A – SUBMISSIONS	**4**
2	What Is Workplace Surveillance?	4
3	Employers Conduct Workplace Surveillance for a legitimate purpose	5
4	Legitimate purpose – Employers comply with OHS laws	5
5	Legitimate purpose – Employers comply with and reduce liability under anti-discrimination laws	8
6	Legitimate purpose – Employers monitor and manage conduct and performance	9
7	Legitimate purpose – Employers must keep records	12
8	Regulation of Workplace Surveillance in Victoria	14
	PART B - TERMS OF REFERENCE	**22**
9	[TOR 1] Effectiveness of privacy & workplace laws	22
10	[TOR 2] Disclosing the use of surveillance	23
11	[TOR 3] Collection, sharing, storage, disclosure, disposal and sale of surveillance data	23
12	[TOR 4] Ownership of surveillance data	23
13	[TOR 5] Protection of privacy, autonomy and dignity, and privacy and data security risks	23
14	[TOR 6] Impacts of surveillance on workers	24
15	[TOR 7 and 8] Impacts on workplace relations, balance of power and workers' rights	25
16	[TOR 9] Examples of best practice regulation	25
17	[TOR 10] Consequences of unregulated surveillance on workers and families	26
18	[TOR 11] Obligations under international law	26
19	[TOR 12] Interaction of state and commonwealth laws, and jurisdictional matters	29
	PART C – CONCLUSION	**30**

1. INQUIRY INTO WORKPLACE SURVEILLANCE

1. The Australian Industry Group (**Ai Group**) appreciates the opportunity to provide this submission to the Victorian Legislative Assembly Economy and Infrastructure Committee (**Committee**) inquiry into Workplace Surveillance (**WS**).[1]

2. Ai Group is a peak national employer organisation representing traditional, innovative and emerging industry sectors. We have been acting on behalf of businesses across Australia for 150 years. Ai Group and partner organisations represent the interests of more than 60,000 businesses employing more than 1 million staff. Our membership includes businesses of all sizes, from large international companies operating in Australia and iconic Australian brands to family-run SMEs. Our members operate across a wide cross-section of the Australian economy and are linked to the broader economy through national and international supply chains. We make this submission to the Inquiry on behalf of our members.

3. We consider it reasonable and appropriate for the Victorian Government to inquire into the extent to which surveillance data is being collected, shared, stored, disclosed, sold, disposed of and otherwise utilised in Victorian workplaces.

4. It is our submission that:

   a. Employers who engage in workplace surveillance generally do so for legitimate and lawful reasons.

   b. The current regulatory framework of Victorian and Commonwealth privacy, workplace surveillance, occupational health and safety (**OHS**) and workplace relations laws are effective and together operate to ensure that employee workplace surveillance is conducted in a fair and appropriate manner.

   c. No changes should be considered by the Victorian Government until the Commonwealth Government review of the Privacy Act 1988 (Cth) (Privacy Act) and related amendment legislation has been finalised.

[1] Parliament of Victoria Inquiry into workplace surveillance (parliament.vic.gov.au) Retrieved, July 2024.

d. If, despite our submissions, the Committee supports the making of any changes, they should be limited to developing best practice non-legislative guidelines in collaboration with employees, employers and their representatives. Guidelines have the advantage of being able to be dynamic, to be rapidly introduced following consultation and co-development, and allowing prompt changes where technologies or practices change.

5. We set out the detail of our submissions below.

PART A- SUBMISSIONS

2. WHAT IS WORKPLACE SURVEILLANCE?

6. As set out in the media release / online announcement launching this inquiry[2] 'workplace surveillance' may take many forms, but broadly falls under four categories: optical, data, tracking and listening. This categorisation continues to be relevant in the contemporary workplace and is adaptable to new and emerging technologies.

7. Workplace surveillance includes (but is not limited to):

   a. Video and audio surveillance, such as CCTV or microphones.

   b. ICT surveillance3, including surveillance of email and internet use, internal company intranets, mobile telecommunications, apps, and onsite electronic communications such as two-way radios.

   c. Tracking surveillance, including tracking employee locations within workplaces and the locations of vehicles, such as GPS tracking.

8. Different forms of workplace surveillance may be used in combination, such as a camera being installed in the cabin of a vehicle, or communications technologies also providing location data.

9. In this submission, for ease of reference, we refer to 'workplace surveillance' as 'WS'.

[2] Parliament of Victoria (11 June 2024) 'Data care key part of workplace surveillance inquiry'.
[3] Information and Communications Technology (ICT).

3. EMPLOYERS CONDUCT WORKPLACE SURVEILLANCE FOR A LEGITIMATE PURPOSE

10. Victorian employers conduct WS for sound, lawful and legitimate purposes, including to support business operations, to deter damaging or unlawful conduct by its workers or customers/clients and to comply with legal obligations.

11. WS assists employers in:

    a. complying with legal obligations under occupational health and safety (OHS) laws, including taking steps to prevent or eliminate risks of physical or psychological injury to workers and others in the workplace;

    b. complying with legal obligations under anti-discrimination and equal opportunity legislation to prevent sexual or gender-based harassment and other related behaviours in the workplace and to minimise vicarious liability;

    c. reasonably monitoring and managing worker misconduct or poor performance; and

    d. complying with employment record-keeping requirements under the Fair Work Act 2009 (Cth) (**FW Act**).

12. It is of vital importance that employers are not constrained by surveillance legislation from complying with other workplace laws such as, OHS laws, anti-discrimination legislation (including taking reasonable steps to prevent sexual harassment), workplace relations legislation as it applies to managing misconduct or underperformance and legislation requiring record-keeping on working hours.

4. LEGITIMATE PURPOSE – EMPLOYERS COMPLY WITH OHS LAWS

13. An employer's use of WS for the purpose of ensuring the health and safety of workers and others in the workplace is legitimate. An employer's ability to utilise it for such purposes should not be unduly impinged upon.

14. OHS laws require employers to identify hazards in the workplace which create (or which may create) risks to the health and safety of others in the workplace.

15. Employers must implement measures to eliminate risks to health and safety caused by those hazards so far as is reasonably practicable and, if elimination is not reasonably practicable, the organisation must minimise the risks associated with the hazards so far as is reasonably practicable

16. WS provides employers with information to control risks and has significant potential to assist employers and employees in improving workplace safety.

17. Surveillance based safety technologies are creating new opportunities to identify risks and manage hazards. For example:

    a. The use of 'wearables' by employees to monitor location, health indicators, and potential exposures to hazards.[4] This includes technology such as:

        (i) A glove that monitors strain and potential injury and allows "real-time personal haptic coaching to reduce workers' risk exposure".[5]

        (ii) New technology being used to understand and control dust exposures through wearable sensors, with a focus on supporting risk minimisation.[6] This technology monitors compliance with policies and builds intelligence and insights, it also helps employees monitor `their own exposures'.

    b. Using data gathered through WS to make ergonomic improvements.

    c. Surveillance via mobile phones offering new mechanisms to ensure employees working alone can be properly monitored to ensure their safety, including in unpredictable environments.[7]

    d. Newer surveillance technologies also alerting employers to near misses which could have caused injuries and providing data to analyse and minimise such

[4] See Real-time Safety Monitoring - XMPRO.
[5] See Australia | Inteliforz™ - Connected Workplace Solutions by Ansell.
[6] See gcg.net.au/wp-content/uploads/2023/09/ExposiAnimation_wSubtitles.mp4.
[7] See Direct Safety's range of cellular personal safety devices enhance the overall safety of lone workers | Direct Safety, Australia & New Zealand (directsafetygroup.com).

risks in future.[8] [9]

e. Road safety being informed by surveillance data10 and recent innovations in tracking technologies providing employers running fleets of vehicles with advanced tracking, journey management, compliance support, and video telematics.[11] [12]

18. There has been extensive discussion of the positive role AI may play in OHS.[13]

> "By leveraging technologies such as machine learning, natural language processing, and visual technology, AI systems can efficiently collect and analyze safety incident data. These systems are capable of scanning data streams for early signs of equipment failure, assessing hazards, and generating strategies to mitigate them. This comprehensive approach ensures that safety incidents, including near misses, are detected, analyzed, and reported with minimal human intervention, significantly reducing the risks associated with underreporting".[14]

19. This last point is particularly relevant. WS is being used, jointly with AI to overcome non-reporting, by both employees and line supervisors.

20. WS is reducing the human or discretionary element of safety supervision and monitoring and ensuring more comprehensive empirical feedback into measures to improve workplace safety.

21. It would be extremely detrimental if changes were made to WS laws which denied Victorian employees and employers the OHS benefits that can come from:

a. Being able to utilise and apply WS innovations, including linkages between WS information and AI.

b. The ability to use the learnings from WS to implement high order controls that eliminate or minimise risk, by redesigning work and the environment.

---

[8] Valerio Elia et al. (2022) 'Applications of smart technologies for automatic near miss detection in the industrial safety', Procedia Computer Science 200 (2022) 1282–1287.
[9] See The Fundamentals of 24/7 Vehicle Near-Miss Detection: Enhancing Safety in Real-Time | Protex AI.
[10] See Near Miss Technology: Saving lives with data insights - VivaCity (vivacitylabs.com).
[11] See MiX Fleet Manager Premium - MiX by Powerfleet Australia (mixtelematics.com).
[12] See What Is Telematics? - Transport Certification Australia (tca.gov.au).
[13] See From Chaos to Clarity: Mastering Health & Safety Data with AI Key Takeaways | Protex AI Company website blog
[14] See The Role of AI in Near Miss Reporting (securade.ai).

c. The application of WS to ensure compliance with policies and procedures designed to improve workplace safety.

22. WS laws as they are support Victorian employers and employees to more effectively comply with OHS laws.

5. LEGITIMATE PURPOSE – EMPLOYERS COMPLY WITH AND REDUCE LIABILITY UNDER ANTI-DISCRIMINATION LAWS

23. It is a legitimate purpose for employers to use WS to comply with and reduce liability under anti-discrimination and related laws for inappropriate workplace behaviour.

24. Employers have a positive duty to take reasonable and proportional measures to eliminate the unlawful sex discrimination, sexual harassment, sex-based harassment, conduct which creates a hostile workplace environment on the ground of sex and related victimisation as far as possible in the workplace under the Sex Discrimination Act 1984 (Cth).

25. There is a similar positive duty under the Equal Opportunity Act 2010 (Vic) which also applies to discrimination in respect of all prescribed protected attributes.

26. There is also a co-existing and separate positive duty which requiring organisations to take proactive action to prevent the risk of harm to workers from psychosocial hazards under OHS laws in Victoria. Behaviours subject to the positive duties under anti-discrimination and equal opportunity legislation are also psychosocial hazards.

27. Separate to the positive duties referred to above, workers can seek individual legal redress (including financial compensation) if they have been unlawfully discriminated against or have been harassed in the workplace in relation to prescribed characteristics. Relevantly, if an employee or agent unlawfully discriminates or harasses another employee in connection with their duties and their employer has not taken ‘reasonable steps’ to prevent that happening, the employer may be taken to have done that act and will potentially be liable for the employee’s unlawful behaviour. It is in an employer’s interests to also mitigate the risk of being vicariously liable.

28. The FW Act also prohibits unlawful discrimination and sexual harassment at work. Workers may access dispute resolution for unlawful sexual harassment in the Fair

Work Commission (**FWC**), including seeking relevant orders such as for compensation from a Court (which the employer may be liable for if they have not taken 'reasonable steps'), and/or stop bullying or stop harassment orders. General protections remedies may also be available if there is unlawful discrimination.

29. WS is crucial tool in managing the duties and risks related to inappropriate workplace behaviours referred to above.

30. For example, and without limitation, WS may be helpful to:

    a. Deter and monitor for inappropriate workplace behaviour where there are risks of bullying and harassment (e.g. by customers in a store, or in remote, less supervised workspaces).

    b. Assist an employer in conducting investigations into inappropriate or damaging behaviour, for example in response to complaints, and to support remedial or disciplinary action against an employee(s) or third parties.

    c. Moderate communications using technology to ensure that technology is not used to perpetrate unlawful workplace behaviour.

6. LEGITIMATE PURPOSE – EMPLOYERS MONITOR AND MANAGE CONDUCT AND PERFORMANCE

31. It is a legitimate purpose for employers to use WS to monitor and, if required manage the employees' conduct or performance.

32. This has a two-fold purpose.

    a. First, it is an exercise of an employer's prerogative to manage its workforce.

    b. Secondly, it is recognised that employers can be liable for their employees' conduct when they use ICT (or any other technology) in the workplace.

33. Industrial courts have recognised this legitimacy of such practices, including by endorsing employers monitoring the email and internet use of employees to identify inappropriate material or conduct.

34. In *Re Queensland Rail* (2006) 156 IR 393 a Full Bench of the Australian Industrial Relations Commission (AIRC) (a predecessor to the FWC) stated at [3]:

> "It cannot be doubted that electronic traffic in sexually related, pornographic and violent images is of legitimate and growing concern to employers. Such images, apart from being offensive to many, can undermine acceptable standards of behaviour in the workplace and create an environment conducive to harassment and discrimination. It is possible, even likely, that an employer which does not take active steps to eliminate traffic of this kind on its email and other electronic communication systems may incur legal liability, under anti-discrimination legislation for example. It is reasonable and, arguably, necessary that employers take what steps they can to eradicate traffic in such images."

35. While it is accepted that an employer has a reasonable basis to monitor, for example, ICT use, industrial courts have also recognised that, in considering whether a dismissal is harsh, unjust or unreasonable, consideration should be given to whether an employee was aware, and understood the nature, of surveillance being conducted. This then also regulates the fairness and appropriateness of WS when used to monitor employee conduct and performance in the workplace.

36. In considering whether inappropriate conduct captured through WS activity justifies dismissal, industrial courts have had regard to whether:

    a. The employer has a workplace policy making it abundantly clear what is appropriate, and inappropriate, behaviour on the employer's computer systems.

    b. The workplace policy details how the employer will monitor compliance with the policy, for instance the type, nature and level of monitoring, and that the employer acts in accordance with its policy.

    c. The employer has appropriately disseminated the policy, and employees are aware of the workplace policy and its implications.

    d. Warnings are provided that a breach of the policy can lead to disciplinary consequences, including dismissal.

    e. Employees are trained on the policy and understand the scope of its application, including the potential for out-of-hours activities to be covered where they have a relevant nexus to the employment relationship, and the

potential for an employee's activity on email and internet to be discoverable by an employer even after the employee has deleted the content.

37. The FWC has determined unfair dismissal claims where employers act on the basis of information obtained through WS, including telephone recordings between employees.[15] Such decisions further underscore the importance of employers having clear policies on WS, and using terms in written employment contracts and other such measures to make it clear to employees that they are subject to surveillance, and to have employees agree to such arrangements as terms of their employment and the basis upon which they use the employer's property and resources.

38. Relevantly also, surveillance material will generally need to be legally obtained in order to be admissible in a court. Under section 139 of the *Evidence Act 1995* (Cth), a court has the discretion to exclude evidence that was obtained improperly or in contravention of an Australian law, unless the desirability of admitting the evidence outweighs the undesirability of admitting the evidence. A court has the discretion to admit the evidence after it has considered a number of matters, including the probative value of the evidence and the gravity of the contravention. This ensures that employers do not undertake WS in an unregulated or unlawful manner.

39. In the context of the FW Act, s.551 confirms that courts are bound by rules of evidence and procedures for civil matters when hearing proceedings for a contravention of civil remedy provision of the FW Act (for instance, adverse action provisions). By comparison, s. 591 of the FW Act provides that the Fair Work Commission (**FWC**) is not bound by the rules of evidence in relation to a matter before it, such as an unfair dismissal claim. However, a fair and appropriate response to the use of WS data is also achieved by the FWC as, when it has regard to the evidence to determine if a dismissal is harsh, unjust or unreasonable, it will consider whether there has been procedural fairness and this may include a consideration of the manner in which the conduct was detected by an employer (i.e., including where WS was used).

40. WS is also able to be addressed in bargaining and to give rise to disputes before the FWC, including disputes under dispute settlement clauses in enterprise agreements.

[15] E.g. Terrence McGlashan v MSS Security Pty Limited [2022] FWC 3304,

An example of recent WS clauses in an enterprise agreement is as follows:

"9.13 TECHNOLOGY

9.13.1 To assist in the company's commitment to health and safety, security of company assets and reduce the Employer's insurance premiums the Employer may install monitoring and surveillance equipment, including GPS, at the workplace and in company vehicles.

9.13.2 Prior to the Employer installing such equipment they shall inform the employees in writing, by posting a notice al the workplace. The written notice will state the type of equipment being installed and the date/s of the installation. The company will then enter into a period of consultation with the workforce to help identify issues of concern with the implementation of new technology into the day-to-day operations of the company. This consultation may include but not be limited to discussion around training, security and changes to current work methods. This period of consultation should be no less than one month."[16]

41. This is not necessarily the best example, or in the terms many employers would seek for such an agreement clause, but it illustrates that WS is also addressed in agreement making under existing workplace relations legislation and that it is accepted as being mutually beneficial by employers, employees and their representatives.

42. Notably, the ACTU supported regulating employee privacy considerations through negotiated collective agreements in its submission to the Privacy Act Review.[17]

7. LEGITIMATE PURPOSE – EMPLOYERS MUST KEEP RECORDS

43. An employer is required to keep certain records for compliance purposes and may also keep employee records for best practice reasons.

Required records

44. An employer must make, and keep for seven years, correct employee records of the kind prescribed in the Fair Work Regulations (section 535, FW Act).

45. If required, an employer must provide access to those records for inspection and auditing, including by Fair Work Inspectors.

[16] GNB Energy Pty Ltd and CEPU Electrical Division Cross River Rail Project Agreement 2020-2024.
[17] (2022) Privacy Act Review Report 2022, p.70, citing the ACTU's Submission to the Review

46. The FW Act defines employee records as something that is an employee record, in relation to the employee, for the purposes of the Privacy Act (section 12, FW Act).

47. However, as the definition of employee records is broad, the FW Regulations sets out the specific kind of employee records that employers must keep to satisfy the record-keeping requirement under s.535, which includes the following:

    a. basic employment details such as the name of the employer and the employee and the nature of their employment (e.g., part-time, full-time, permanent, temporary or casual);

    b. pay;

    c. overtime hours;

    d. averaging arrangements;

    e. leave entitlements;

    f. superannuation contributions;

    g. termination of employment (where applicable); and

    h. individual flexibility arrangements and guarantees of annual earnings.

48. Employee records are private and confidential. Only the employer, payroll staff, the employee and authorised individuals, such as an accountant, can access the records.

<u>Best practice records</u>

49. Subject to the SD Act and the Privacy Act, employers may otherwise retain data relating to employees during employment and then for period after, as is required:

    a. for legislative and compliance purposes; or

    b. for so long as they determine necessary based on their judgements of possible compliance risks and requirements – including future legal claims.

50. No employer should be placed in a position of facing future litigation which could have been clarified by WS information that has been gathered but cannot used be due to forced data disposal.

51. We have seen in relation to casual employment across the past decade employers quite unexpectedly face claims that they have underpaid casual employees and purported liabilities extending back further than the standard seven years for employee records retention under the Fair Work Act.

52. We also see exercises in discovery in a wide range of litigation that makes it important to retain emails for an extended period of time.

53. If WS data is handled appropriately, and retained within organisations, it should be able to be retained for so long as an employer considers it prudent to do so. A lack of corroborative information where records have been forced to be disposed of should not stop employers from defending matters that WS data would have clarified.

8. CURRENT WORKPLACE SURVEILLANCE IN VICTORIA

54. We consider the area of workplace surveillance to be already comprehensively regulated for Victorian employers.

Surveillance Devices Act 1999 (Vic)

55. The Surveillance Devices Act 1999 (Vic) (**SD Act**) regulates the installation, use and maintenance of listening devices, optical surveillance devices, tracking devices and separately, and the use of data surveillance by law enforcement officers.

56. The SD Act is backed by the potential for high fines, criminal conviction and imprisonment.

57. The SD Act is suitable to the contemporary ways of working (including remote and home-based working) as it:

    a. not only regulates employees, but extends that regulation to other workers, including:

        i. a person under a contract for service (i.e., an independent contractor);

ii. a person who performs work which is remunerated wholly or partly on commission; and

iii. a person who performs work on an unpaid or voluntary basis; and.

b. defines the '*workplace'* as "any place where workers perform work".

58. The SD Act Prohibits WS in bathrooms, washrooms etc.[18]

a. Prohibits WS in bathrooms, washrooms etc.[19]

b. Requires express or implied consent to the use of WS devices.20

c. Imposes various penalties for non-prescribed surveillance.

d. Regulates workplace privacy in certain areas of the workplace.21

e. Restricts communication and publication of private conversations and activities made with certain WS devices.22

f. Generally, prohibits covert surveillance (i.e., without consent) and prescribes a process of surveillance authorisation and monitoring

59. The SD Act is sufficiently broad in scope to account for advancements in technology which underpin a contemporary workplace.

60. As discussed below, when considered in conjunction with the Privacy Act 1988 (Cth), there is already an adequate and robust regulation of WS in Victoria. There is not the regulatory omission in Victoria suggested by the initial framing of this inquiry.[23]

Interaction between the SD Act and the Privacy Act

61. The SD Act should not be viewed as a sole source of surveillance legislation.

62. Many Victorian employers are also regulated by the Privacy Act and associated

[18] Surveillance Devices Act 1999 (Vic), s.9B.
[19] Surveillance Devices Act 1999 (Vic), s.9B.
[20] E.g. Surveillance Devices Act 1999 (Vic), s.8.
[21] E.g. Surveillance Devices Act 1999 (Vic), Part 2A.
[22] E.g. Surveillance Devices Act 1999 (Vic), Part 3.
[23] Victoria's workplace surveillance inquiry to look at data handling (parliament.vic.gov.au)

Australian Privacy Principles (**APPs**), subject to relevant exemptions relating to small business and employee records. The Privacy Act and APPs also apply to individual persons and not just employees – i.e., including independent contractors etc.

63. The Privacy Act and its associated 13 APPs are also relevant to workplace surveillance regulation. The Privacy Act and APPs are enforced by an established regulator, the Office of the Australian Information Commissioner (**OAIC)**.

64. The Privacy Act and APPs contain some important exemptions for employers. They do not apply to employers who meet the small business threshold exemption of an annual turnover of $3 million (**the small business exemption**).

65. In addition, the Privacy Act currently provides an exemption under ss. 7(1)(ee) and 7B(3) for acts done or practices engaged in by an organisation that is or was an employer of an individual if the act or practice is directly related to:

    a. a current or former employment relationship between the employer and the individual; and

    b. an employee record held by the organisation and relating to the individual.

66. Accordingly, the APPs are relevant to Victorian entities engaging in workplace surveillance where those Victorian entities do not meet the small business exemption or where the surveillance acts or practices are outside the employee records exemption.

67. In these circumstances, it is useful to highlight those APPs that are relevant to ‘workplace surveillance’ and may potentially possess some overlap with the provisions of the WS Act in respect of the range of restrictions on whether and how information obtained from surveillance is to occur.

68. APP 3 concerns the solicitation and/or collection by an entity of personal information and imposes restrictions on when and how this must be done. Generally, APP 3 restricts the collection or solicitation of personal information to where it reasonably necessary, or directly related to, one or more of its functions or activities.

69. The OAIC's guide to the APPs states that the concept of 'collection' applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means, including from:

    a. individuals

    b. other entities

    c. generally available publications

    d. surveillance cameras, where an individual is identifiable or reasonably identifiable

    e. information associated with web browsing, such as personal information collected by cookies

    f. biometric technology, such as voice or facial recognition

70. APP 3.3 imposes an additional requirement for collecting sensitive information about an individual, being where the collection must be reasonably necessary for one or more of the entity's functions or activities and where the individual about who the sensitive information relates consents to the collection.

71. There are some exceptions to when the additional requirement for collecting sensitive information about an individual applies. These are generally limited to specific reasons including:

    a. where collecting sensitive information is required or authorised by law;

    b. where a permitted general situation exists of which there are seven categories (including, lessening or preventing a serious threat to life, health or safety; taking appropriate action to address unlawful or serious misconduct; or to establish or defend a legal or equitable claim);

    c. where a permitted health situation exists;

    d. for an enforcement related activity; and

e. for not-for-profit organisations.

72. APP 3 also imposes requirements on the collection of sensitive information such that sensitive information is to be collected personally from the individual unless it is unreasonable or impracticable do so, or the individual consents to somebody else providing the information.

73. Sensitive information is defined by the Privacy Act as meaning:

a. information or an opinion about an individual's:

i. racial or ethnic origin; or
ii political opinions; or
iii. membership of a political association; or
iv religious beliefs or affiliations; or
v philosophical beliefs; or
vi membership of a professional or trade association; or
vii membership of a trade union; or
viii sexual orientation or practices; or
ix criminal record,

that is also personal information; or

b. health information about an individual; or

c. genetic information about an individual that is not otherwise health information; or

d. biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

e. biometric templates.

74. This definition combined with the broad term 'collection', including various types of potential workplace surveillance referred above, demonstrates that there are strong restrictions on whether and how an employer can conduct workplace surveillance under the Privacy Act, assuming the employee records exemption and small business exemption do not apply.

75. In addition, APP 5 requires entities to take reasonable steps to provide specific notification disclosures to individuals about whom the entity collects personal information from. The notification must be made before or at the time of the collection. If this is not practicable, reasonable steps to notify must be taken as soon practicable after the personal information has been collected.

76. Under APP 6 an entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies. A range of exceptions apply, including where a person has consented to the disclosure for that secondary purpose; where the disclosure for the secondary purpose if required or authorised by a law or order from a Court or Tribunal; and where the disclosure for the secondary purpose relates to the primary purpose and the person reasonably expects the disclosure to be made.

77. It is therefore essential that the SD Act is not seen as the sole source of regulation on workplace surveillance for Victorian employers, nor viewed as limited in its scope in regulating surveillance over those persons or workplace circumstances that may be outside the coverage of the SD Act.

The Privacy Act Review

78. On 30 October 2020, the Commonwealth Government commenced a major review of the Privacy Act 1988 (Cth) (**Privacy Act Review**).[24]

79. On 16 February 2023, the Australian Government released its Privacy Act Review Report following its review of the Privacy Act. Ai Group participated in the review's consultation process and lodged several submissions seeking, amongst other things, to maintain existing exemptions for small business and for employee records.

80. The Privacy Act Review Report contains a number of privacy reforms proposed by the Federal Government. These included several recommendations that impact workplaces, the employment relationship and how WS is regulated, such as:

    a. The removal of the small business exemption from the application of the Privacy Act and the APP but only after an impact analysis has been undertaken to show

[24] Review of the Privacy Act 1988 | Attorney-General's Department (ag.gov.au).

the impact on small business and to identify the necessary support measures needed.

> "In recognition of the increasing privacy risks posed by small businesses and the benefits of improved privacy protection for Australians and the economy, the small business exemption should be removed. This would require all Australian businesses to comply with the Act, regardless of annual turnover".[25]

b. Proposing that further privacy protections be given in relation to employment information covered by the employee records exemption, including:

   i. better transparency around the collection and use of employee personal information;

   ii. protections to guard against the misuse, loss or unauthorised access to such information, including destroying the information if no longer required;

   iii. obligations on employers to notify both employees and the Information Commissioner upon a data breach likely resulting in serious harm; and

   iv. ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and whether consent should still be required to collect employees' sensitive information.

c. Consideration of how such enhanced privacy protections should be extended to private sector employees after further consultation between the Federal Government, employer and employee representatives with the aim of:

   > "(a) providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for
   >
   > (b) ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information

[25] Attorney General's Department (2022) Privacy Act Review Report 2022, p.61

(c) ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and

(d) notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm.

Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact. The possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored."[26]

d. Consideration of whether industry codes of practice regarding the collection, use and disclosure of personal information of employees should be explored as part of a tripartite process.

81. On 28 September 2023, the Commonwealth Government released its response to the Privacy Act Review Report.[27] To date amending legislation has not been introduced into the Australian Parliament, but it is expected it will be in due course.

82. AI Group's input to the Commonwealth's Privacy Act Review[28] centred on various themes that are directly relevant to the Committee's current inquiry, including:

a. The need for evidence-based policy making, and properly understanding phenomena and possible approaches to them prior to making any recommendations for change, particularly for additional prescription or regulation.

b. The need to properly understand and evaluate any options under consideration.

c. Avoiding excessive, overly burdensome, or overlapping regulation.

d. The need to properly understand the priorities and concerns of those targeted for protections, in this case of employees, without undue or damaging assuming regarding their interests or priorities.

[26] Attorney General's Department (2022) Privacy Act Review Report 2022, p.71
[27] Government response to the Privacy Act Review Report | Attorney-General's Department (ag.gov.au), September 2023.
[28] Ai Group (2020) Submission to the Australian Government Attorney-General's Department, Review of the Privacy Act 1988

e. The need to support industry in meeting changed or extended obligations, and to identify and evaluate any additional compliance costs.

f. The importance of thoughtful strategy and credible policy responses that allow businesses to plan for and respond to economic and technological change in ways that will meet community expectations, rather than overly limiting future innovation.

g. The importance of identifying, promoting and supporting the adoption of best practice approaches.

h. The importance of collaboration in effectively executing any changes of policy and regulation.

83. Ai Group continues to represent employers as part of the Federal Government's ongoing consultations on how the Report's recommendations should be implemented.

84. In light of this the Committee should:

a. Recognise the potential impact of pending changes in Commonwealth privacy law to the regulation of WS, and that such changes are expected to be introduced.

b. Recommend Victoria not seek to take any additional or changed actions on WS prior to the introduction and passage of Commonwealth Privacy Act amendments.

PART B – TERMS OF REFERENCE

9. [TOR 1] EFFECTIVENESS OF PRIVACY & WORKPLACE LAWS

85. The first Term of Reference asks the Committee to consider 'The effectiveness of current privacy and workplace laws when it comes to employee workplace surveillance'.

86. We restate our submissions above. The current privacy, workplace and WS laws apply effectively to employee workplace surveillance.

10. [TOR 2] DISCLOSING THE USE OF SURVEILLANCE

87. The second Term of Reference asks the Committee to consider 'The current practices of employers disclosing the use of workplace surveillance to employees and others'.

88. We refer to our submissions above in relation to the keeping employee records. Employers do not disclose data in relation to workplace surveillance except as permitted or required by law.

11. [TOR 3] COLLECTION, SHARING, STORAGE, DISCLOSURE, DISPOSAL AND SALE OF SURVEILLANCE DATA

89. The third Term of Reference asks the Committee to consider '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.'

90. We refer to our submissions above. Employers use WS data for legitimate purposes and as permitted or required by law.

12. [TOR 4] OWNERSHIP OF SURVEILLANCE DATA

91. The fourth Term of Reference asks the Committee to consider 'The ownership of workplace surveillance data'.

92. These activities are regulated by the Privacy Act and, depending on the data, may also be regulated by bespoke record-keeping requirements under the FW Act, contractual arrangements or confidentiality laws.

93. We refer to our submissions above, particularly in relation to the Privacy Act. Employers comply with the Privacy Act and any other relevant laws, including relating to confidentiality and privacy of data, in relation to data collected by WS.

13. [TOR 5] PROTECTION OF PRIVACY, AUTONOMY AND DIGNITY, AND PRIVACY AND DATA SECURITY RISKS

94. The fifth Term of Reference asks the Committee to consider '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'.

95. We note the Commonwealth Government is currently consulting on its Australian Cyber Security Strategy: Legislative Reforms – 2023-2030. Ai Group is engaged in this consultation and agrees there is a need for new cyber security legislation to be developed to support the objectives of the National Cyber Security Strategy. However, regulatory measures adopted as part of this legislative agenda must consider the balance between cyber security and business innovation and digitisation. It is imperative that regulation be supportive of the efforts by industry to enhance its cyber capabilities. Regulation must be designed in a way that is practical for widespread uptake amongst industry, imposes least-cost compliance burden, and supports rather than inhibits confidence in broader digital upgrading by industry. Businesses (and employers) facing cyber-attacks are victims of a crime and must be treated as such. Punitive measures must be directed at the perpetrators of crimes, not the victims.

96. It is out of scope for WS Victorian laws to address cyber security given that this is already forming part of a developing Commonwealth Government legislative agenda.

97. We refer to submissions above which demonstrate how employers use WS data fairly and appropriately, consistent with expectations under the SD Act, Privacy Act, OHS laws and workplace relations laws.

14. [TOR 6] IMPACTS OF SURVEILLANCE ON WORKERS

98. The sixth Term of Reference asks the Committee to consider 'the personal impact of workplace surveillance on Victorian workers, such as on their physical and mental safety'.

99. We refer to our submissions above which emphasise that employers have duties under OHS laws to ensure the physical and psychological health and safety of workers and others in the workplace. WS assists employers in complying with this duty and cannot be used in a manner that would create risks to workers health and safety.

15. [TOR 7 AND 8] IMPACTS ON WORKPLACE RELATIONS, BALANCE OF POWER AND WORKERS RIGHTS

100. The seventh Term of Reference asks the Committee to consider 'The impact of workplace surveillance on workplace relations and the balance of power between employers and workers', and the eighth Term of Reference queries 'The impact of workplace surveillance on the balance of power in the workplace and the effect on workers' rights.

101. We refer to our submissions above which demonstrate that the industrial courts are more than capable of balancing employer and employee rights in the workplace to ensure that WS cannot be used to adversely affect the balance of power in the workplace nor to erode workers' rights. The Privacy Act currently also supports workers' rights and any changes made through the current review will further enhance this support – at least from the perspective of employees in the workplace.

16. [TOR 9] EXAMPLES OF BEST PRACTICE REGULATION

102. The ninth Term of Reference asks the Committee to consider 'International or domestic examples of best practice workplace surveillance regulation and privacy protection'.

103. We welcome this consideration. Ai Group's primary recommendation is that promoting and supporting best practices form the heart of future approaches to the use of WS in Victorian workplaces. Non-binding guidelines, backed by examples of good practices will be of most assistance and impact in equipping Victorian employers and employees to positively and effectively use WS to respond to contemporary challenges and regulatory demands.

104. Best practice WS regulation lies in encouraging, promoting and supporting the application of best practices in workplaces, and encouraging positive relations between employers and employees in relation to WS.

105. Guidelines and support, rather than prescriptive regulation, will provide the most effective foundations for delivering best practices.

106. Best practice guidelines should be co-developed through tripartite engagement with employer and union representatives, rather than imposed solely by government.

107. We also refer the Committee to our submissions above, including in relation to the Privacy Act and its review.

17. [TOR 10] CONSEQUENCES OF UNREGULATED SURVEILLANCE ON WORKERS AND FAMILIES

108. The tenth Term of Reference asks the Committee to consider 'The potential consequences of unregulated surveillance on workers and their families'.

109. We refer to our submissions above. If employers conduct WS, it is regulated effectively through the SD Act and Privacy Act, and also by the industrial courts through workplace relations laws. WS may only be used in a manner which does not create risks to the health and safety of workers and others.

18. [TOR 11] OBLIGATIONS UNDER INTERNATIONAL LAW

110. The eleventh Term of Reference asks the Committee to consider 'Australia's obligations under international law, including International Labour Organization (ILO) Conventions'.

111. The ILO is not an at large authority pronouncing how workplaces should be regulated, save when its annual International Labour Conference (ILC) formally adopts new international labour standards. Relevantly:

    a. Even within the body of ILO standards, it is only Conventions which can be ratified and thereby give rise to treaty obligations in Australia. Australia has ratified 60 of 191 ILO Conventions.[29]

    b. Where ratification occurs, it becomes an obligation of the Commonwealth Government to bring Australia's domestic law and practice into conformity with

[29] A number of which are no longer in force. Australia has also ratified two optional protocols.

an ILO convention, and to confirm and report on our compliance with the requirements of the convention on an ongoing basis.[30]

c. As a federal state, these obligations may be met in whole or part by state and territory legislation, which the Commonwealth reports upon to the ILO and its supervisory mechanisms. For example, Australia's obligations under ILO Convention 111 are met by both Commonwealth and state legislation on workplace relations and anti-discrimination.[31] Obligations under Convention 155 are met by state, territory and Commonwealth OHS laws.[32] The relevance of this is that if Australia had international obligations on WS of the type referred to in TOR 11, we would have already seen comprehensive WS legislation at commonwealth level or in all states and territories.

d. In fact, Australia would not have ratified an ILO convention on WS, were one to exist, unless our domestic law and practice already complied with its requirements. Thus, this consideration could not be used to justify any change in the law in Victoria. Were international obligations applicable and were they to dictate changes to the law in Victoria, this would already have occurred prior to Australia ratifying any ILO standard.

112. However, there is no such ILO standard, and no ratifiable convention on WS or the privacy of employment related data. Australia has no direct or specific ILO obligations regarding the focus of this inquiry.

113. Confusion can occur between ILO obligations and the wider research undertaken by the ILO bureaucracy[33], and experts' meetings, which do not create treaty obligations on ILO member states. There are research papers for ILO experts' meetings, and some of these meetings adopt conclusions, but these provide interesting analysis, rather than rising to the level of norms or ratifiable treaties. The normative standards

[30] The obligations are a little more complex than this, and some arise from the ILO Constitution and ILO membership, rather than specific ratifications, but these are not directly related to surveillance.
[31] C111 - Discrimination (Employment and Occupation) Convention, 1958 (No. 111).
[32] C155 - Occupational Safety and Health Convention, 1981 (No. 155).
[33] Which is quite specifically not the normative standards of the ILO. In practice the academic of the research of the ILO Office (through the bureaucracy) can precede standard setting and is a precursor to consideration by tripartite social partners. It should not however be mistaken for the product of social dialogue.

of the ILO are solely those agreed by the International Labour Conference.

114. An ILO experts' meeting created guidelines on the protection of workers' personal data in 1997, more than 25 years ago.[34] However:

a. This does not appear to have been progressed further or returned to in the intervening years.

b. In more than 25 years, the ILO has not turned this experts' level discussion into normative standard setting, which is the organisation's natural sequence of work if a topic is to progress within the ILO.

i. Each experts' meeting reports to the Governing Body of the ILO for consideration of whether the matter concerned should be included on the agenda of future International Labour Conferences. The 1997 experts' meeting did not give rise to ILO standard setting on WS or the privacy of employees' personal data.

ii. Also notably, the ILO code of practice itself does not appear to have been updated in the past 27 years.

c. The ILO clarified in 1997 that 'as an ILO code of practice, it has no binding force…'.[35]

d. However, something useful can be taken from the ILO Code of Practice. It may offer a further useful starting point for drafting non-binding guidelines for tripartite development in Victoria between government, and peak union and employer organisations.

115. There are also separate ILO guidelines (again non-binding, and not a ratifiable treaty adopted internationally on a tripartite basis) on "Technical and ethical guidelines for workers' health surveillance".[36] This seems a narrower and more specific consideration than those subject to this inquiry.

[34] ILO Protection of workers' personal data (1 January 1997) webpage and guidelines.
[35] Protection of workers' personal data | International Labour Organization (ilo.org).
[36] Technical and ethical guidelines for workers' health surveillance | International Labour Organization (ilo.org).

116. For completeness it may be argued that obligations regarding WS arise under other general or differently directed ILO standards which Australia has ratified.

117. It would be a concern if any national government allowed widespread surveillance of employee discussions with unions, such that there was an interference with workers' rights to freely associate or collectively bargain under the ILO's fundamental or core conventions.[37] However that's a purely theoretical concern that could be addressed under existing Australian law, such as through complaints of breaches of right of entry obligations, and potentially of the existing Surveillance Devices Act 1999 (Vic).

118. We have also reviewed the ILO's fundamental conventions on Work Health and Safety (Conventions 155[38] and 187[39]). Convention 155 refers to the need to review "evolving effective methods for dealing with" the "situation regarding occupational safety and health and the working environment". This seems a recognition that changing technologies, such as new methods of WS may contribute to better meeting Australia's ILO treaty obligations, in particular by contributing to improved OHS.

19. [TOR 12] INTERACTION OF STATE AND COMMONWEALTH LAWS, AND JURISDICTIONAL MATTERS

119. The twelfth Term of Reference asks the Committee to consider 'The interaction between State and Commonwealth laws, and the jurisdictional limits imposed on the Victorian Parliament'.

120. It is for the Victorian Government or any MLC introducing a Bill to consider the legislative capacities of the Victorian Parliament.

121. Major changes are under consideration at Commonwealth level for privacy law following the Privacy Act Review. We refer to our submissions above which recommend not progressing any change of approach in Victoria, other than in providing non-legislated guidance towards best practice, particularly until it is clear how Commonwealth privacy law may change. Waiting until the Privacy Act 1988 (Cth) is amended would seem prudent in regard to working within the Victorian Parliament's

37 The Freedom of Association and Protection of the Right to Organise Convention, 1948 (No. 87) and Right to Organise and Collective Bargaining Convention, 1949 (No. 98).
38 Convention C155 - Occupational Safety and Health Convention, 1981 (No. 155) (ilo.org)
39 Instrument profile (ilo.org).

legislative capacity.

PART C- CONCLUSION

122. Workplace surveillance and the use of that data in Victorian workplaces is effectively regulated and no legislative action is required. Victorian employers engaging in such activities have legitimate purposes and engage in workplace surveillance for sound and lawful reasons, including to ensure the health and safety of workers, to reasonably monitor and manage their workforces and to ensure compliance with laws and regulations. The industrial courts continue to protect workplace rights and preserve an appropriate balance of power between employers and workers. Concerns expressed relating to data security are a matter for the Commonwealth and are currently dealt with under the Privacy Act and under the current Commonwealth Government's legislative agenda to amend Privacy Act and develop cybersecurity legislation.

ABOUT THE AUSTRALIAN INDUSTRY GROUP

The Australian Industry Group (Ai Group®) is a peak national employer organisation representing traditional, innovative and emerging industry sectors. We have been acting on behalf of businesses across Australia for 150 years. Ai Group and partner organisations represent the interests of more than 60,000 businesses employing more than 1 million staff. Our membership includes businesses of all sizes, from large international companies operating in Australia and iconic Australian brands to family-run SMEs. Our members operate across a wide cross-section of the Australian economy and are linked to the broader economy through national and international supply chains.

Our vision is for thriving industries and a prosperous community. We offer our membership strong advocacy and an effective voice at all levels of government underpinned by our respected position of policy leadership and political non-partisanship.

With more than 250 staff and networks of relationships that extend beyond borders (domestic and international) we have the resources and the expertise to meet the changing needs of our membership. Our deep experience of industrial relations and workplace law positions Ai Group as Australia's leading industrial advocate.

We listen and support our members in facing their challenges by remaining at the cutting edge of policy debate and legislative change. We provide solution-driven advice to address business opportunities and risks.

OFFICE ADDRESSES

NEW SOUTH WALES

Sydney
51 Walker Street
North Sydney NSW 2060

Western Sydney
Level 2, 100 George Street
Parramatta NSW 2150

Albury Wodonga
560 David Street
Albury NSW 2640

Hunter
Suite 1, "Nautilos"
265 Wharf Road
Newcastle NSW 2300

VICTORIA

Melbourne
Level 2 / 441 St Kilda Road
Melbourne VIC 3004

Bendigo
87 Wil Street
Bendigo VIC 3550

QUEENSLAND

Brisbane
202 Boundary Street Spring Hill
QLD 4000

ACT

Canberra
Ground Floor,
42 Macquarie Street
Barton ACT 2600

SOUTH AUSTRALIA

Adelaide
Level 1 / 45 Greenhill Road
Wayville SA 5034

WESTERN AUSTRALIA

South Perth
Suite 6, Level 3 South Shore Centre 85
South Perth Esplanade
South Perth WA 6151

www.aigroup.com.au