

# Ai GROUP SUBMISSION

**Impact of technological and other  
change on the future of work and  
workers in New South Wales**

**Select Committee on the  
Impact of technological  
and other change on the  
future of work and workers  
in New South Wales**

27 June 2022

## *Impact of technological and other change on the future of work and workers in New South Wales*

### **Introduction**

The Australian Industry Group (**Ai Group**) has prepared this short submission in response to the invitation from the Select Committee on the Impact of Technological and Other Change on the Future of Work and Workers in New South Wales (**the Select Committee**) to appear as a witness in the Select Committee's Inquiry in respect of the issues of workplace surveillance and automation.

This submission points out that:

- NSW employers engage in workplace surveillance for sound and lawful reasons.
- Employers should not be constrained by privacy or surveillance legislation from complying with other workplace laws such as, work health and safety (**WHS**) legislation, anti-discrimination legislation (including taking reasonable steps to prevent sexual harassment) and legislation requiring record-keeping on working hours.
- The area of workplace surveillance is comprehensively regulated for NSW employers.
- The *Workplace Surveillance Act 2005* (NSW) should not be viewed as a sole source of surveillance legislation. Many NSW employers are subject to the *Privacy Act 1988* (Cth) (**Privacy Act**) and associated 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.
- It is important that the employee records exemption in the Privacy Act is preserved to enable employers to manage compliance obligations under other laws.
- Automation has grown with the emergence of Industry 4.0 and will continue with the expansion of digital technologies and capability.
- With the rise of automation, employers are increasingly requiring knowledge-based workers armed with digital literacy. Employers also are increasingly rewarding qualitative competencies and values-based behaviour. These attributes are not easily measured by workplace surveillance.

### **Workplace surveillance**

Employers who engage in workplace surveillance, generally do so for sound and lawful reasons. Implementing surveillance is a cost to the business in terms of its installation and operation, in addition to any required time spent in reviewing records and material as may be required.

Workplace surveillance, where it exists, is generally implemented to support the operation of the business; to deter damaging or unlawful conduct by others and mitigate risk (e.g. to prevent sexual harassment at work); and to manage compliance with legal obligations (e.g. workplace and WHS laws).

Employers may rely on a form of surveillance (such as computer surveillance) as part of recording hours of work for the purpose of complying with record-keeping obligations under workplace laws, particularly where such obligations exist for workplaces engaged in remote or hybrid working arrangements and where traditional on-site 'bundy' systems to register attendance at work are not available or inappropriate.

Surveillance may also be relied on to 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 work spaces). Surveillance records often assist employer 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.

Employers generally hire and reward based on competencies and values-based behaviours being qualitative skills that are difficult to measure through surveillance. For this reason most employers do not extensively rely on surveillance as part of evaluating job performance; such data does not provide a complete picture of an employee's skill or behaviour.

### ***Workplace Surveillance Act 2005 (NSW)***

Employers in NSW do not have an unfettered right to implement workplace surveillance. The area of workplace surveillance is comprehensively regulated for NSW employers. The *Workplace Surveillance Act 2005 (NSW) (WS Act)* provides for a range of restrictions and obligations on employers if they wish to carry out workplace surveillance.

The WS Act prevents employers from carrying out workplace surveillance until the required notice has been provided to the affected employees (s.10). Additional requirements are in place for camera surveillance, computer surveillance and tracking. These generally include the requirement that the employer provide detailed written notice to the employee, the content of which must make specific disclosures as required by the WS Act.

The WS Act also prohibits employers from carrying out surveillance using a workplace surveillance device when the employee is not at work for the employer (s.16). An important exception to this is in relation to computer surveillance where the equipment or resources used by the employee are provided by, or at the expense of, the employer.

The use of information obtained from surveillance by employers in respect of surveillance records is also restricted by the WS Act. Section 18 requires employers to ensure that any surveillance record of an employee at work for the employer, not be disclosed or used unless it is for:

- A legitimate purpose related to the employment of employees of the employer or the legitimate business activities or functions of the employer;
- Use in connection with the detection, investigation or prosecution of an offence and the disclosure is to a member or office of a law enforcement agency;
- A purpose that is directly or indirectly related to the taking of civil or criminal proceedings; or
- Aversion of an imminent threat of serious violence to persons or of substantial damage to property as reasonably believed by the employer.

In respect of covert surveillance, section 19 of the WS Act restricts the carrying out of workplace covert surveillance of an employee while the employee is at work unless the surveillance is authorised by a covert surveillance authority. Covert surveillance is generally authorised by a covert surveillance authority for the purpose of establishing whether or not one or more particular employees are involved in any unlawful activity while at work for the employer.

### **Workplace Surveillance Act applies to contemporary ways of working**

Not only does the WS Act comprehensively regulate surveillance by NSW employers in respect of employees (as defined by the WS Act), it is also capable of continued application to evolving remote and hybrid working environments.

The WS Act contains an expansive definition of “at work” (see s.5) that includes not only a workplace of the employer, but “*any other place while performing work for the employer*” that would clearly extend to a worker’s home residence if they were engaged in remote working, or working at another site not owned by the employer, for example, a client site or public place.

In addition, the definition of an ‘employer’, extends to bailors of public vehicles and principal contractors in respect of employees who are bailees of public vehicles or carriers under Chapter 6 of the *Industrial Relations Act 1996* (NSW). Similarly, these workers are included in the WS Act’s definition of ‘employee’, in addition to volunteers.

### **Workplace surveillance and Federal privacy legislation**

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**).

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**).

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 current or former employment relationship between the employer and the individual; and
- an employee record held by the organisation and relating to the individual.

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

Also relevantly, unlike the WS Act, the Privacy Act and APPs generally impose obligations on entities in respect of individual persons rather than limiting protections to employees. This means that, generally, surveillance acts and practices by a NSW employer of contractors or consumers, are likely to attract application of the Privacy Act and APPs notwithstanding they may not be covered by the WS Act itself.

In these circumstances, it is useful to highlight those APPs that are relevant to 'workplace surveillance' and 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.

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 is reasonably necessary, or directly related to, one or more of its functions or activities.

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: (emphasis added)

- individuals
- other entities
- generally available publications
- surveillance cameras, where an individual is identifiable or reasonably identifiable
- information associated with web browsing, such as personal information collected by cookies
- biometric technology, such as voice or facial recognition

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.

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:

- where collecting sensitive information is required or authorised by law;
- 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);
- where a permitted health situation exists;
- for an enforcement related activity; and
- for not-for-profit organisations.

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.

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.

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.

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.

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 is 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.

It is therefore essential that the WS Act is not seen as the sole source of regulation on workplace surveillance for NSW employers, nor viewed as limited in its scope in regulating surveillance over those persons outside the coverage of the WS Act.

### **Australian Government review of the Privacy Act**

Ai Group has been active in advocating employer concerns in the Australian Government's review of the Privacy Act. Ai Group has lodged the following submissions to this review:

- [Ai Group submission, Nov 2020](#)
- [Ai Group submission, Jan 2022](#)

In its submissions, Ai Group strongly opposed any narrowing of the employee records exemption. Handling of employee records is best dealt with under current workplace legislation and employers should not be subject to multiple layers of regulation pertaining to the same subject matter.

Any watering down of the employee records exemption in the Privacy Act is likely to cause significant confusion regarding interaction with existing controls in workplace legislation and would potentially put employers at risk of contravening the Privacy Act in the ordinary course of administering the employment relationship. The pandemic has demonstrated to employers the need to procure information from workers in the form of taking temperatures or ascertaining vaccination status in order to mitigate the risk of spreading the COVID-19 virus. Additional restrictions pertaining to dealing with such information would further discourage employers from taking such reasonable management action.

The personal information of employees is adequately protected by the current scope of the employee records exemption. Employer practices in legitimately obtaining relevant information concerning the employment relationship must not be inappropriately proscribed by the APPs. The employee records exemption should be expanded to encompass prospective new employers and the recipients of labour hire services.

## **Automation**

Digitalisation and automation have moved beyond manufacturing and, where technically feasible, are now transforming sectors involving knowledge-focused work. Rapid technological advancements are changing the way technology and work are linked. As technology develops, digitalisation, robotics and machine learning will impact on activities that currently appear to have a low technical potential for automation. Australia is increasingly influenced by the key emerging technologies of cloud computing, the Internet of Things, big data, blockchain, artificial intelligence and robots; and immersive technology.

Digital transformation will create new markets and new jobs and some existing jobs will be re-designed. Digital transformation and the “Fourth Industrial Revolution” (also known as Industry 4.0) associated with it are the latest in a long line of transformational technological changes, dating back to the first industrial revolution in the eighteenth century (and even earlier).

Each of these waves of technological change has been associated with the replacement or reform of particular industries and occupations. They have created entirely new types of goods and services, industries and occupations. This process is the foundation of growth in economic productivity and underpins rises in incomes and living standards for the whole community over time.



Automation is leading to reallocations of employment between roles, tasks, sectors and regions. Changes to skill requirements in industry are occurring at all levels of the workforce. The workforce needs to be able to operate with emerging new technologies and systems and engage in more complex work and relationships in environments that are constantly changing.

Labour demand is shifting towards higher level and more cognitive skills for which many workers are not adequately trained, and it is contributing to the hollowing out of middle level skill jobs. It is demanding, as a threshold requirement, that all workers have mastered enduring concepts of digital literacy to be enabled to adjust to new ICT.

The new workplace increasingly relies on a more complex operational and organisational structure relating to decision making, coordination, control and support services. This means there are significantly higher demands placed on all members of the workforce in terms of managing complexity and higher levels of abstraction and problem solving. Employees are needing to act more often on their own initiative and be able to organise their own work. Enterprise skills (such as advanced reasoning, design thinking and social interaction) need to be coupled with technical skills to build a broader set of capabilities for application in different environments. While the share of high skill work increases, the share of low-skilled work is decreasing. However low skilled workers will still be required as the digital economy evolves. These workers will have an advantage over machines where they have the capacity to adapt to situations. Machines are less able to react to unexpected circumstances and communicate on that basis.



## ABOUT THE AUSTRALIAN INDUSTRY GROUP

The Australian Industry Group (Ai Group®) is a peak employer organisation representing traditional, innovative and emerging industry sectors. We are a truly national organisation which has been supporting businesses across Australia for nearly 150 years.

Ai Group is genuinely representative of Australian industry. Together with partner organisations we represent the interests of more than 60,000 businesses employing more than 1 million staff. Our members are small and large businesses in sectors including manufacturing, construction, engineering, transport & logistics, labour hire, mining services, the defence industry, civil airlines and ICT.

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. We provide the practical information, advice and assistance businesses need. Our deep experience of industrial relations and workplace law positions Ai Group as Australia's leading industrial advocate.

We listen and we 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, "Nautilus"  
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](http://www.aigroup.com.au)