The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
PO Box 289
North Sydney NSW 2059
Australia
ABN 76 369 958 788

4 November 2024

Legal and Constitutional Affairs Legislation Committee
PO Box 6100
Parliament House
Canberra ACT 2600

By email: legcon.sen@aph.gov.au

Dear Secretariat

Re. Responses to questions on notice

We write regarding our appearance at the hearing before the Legal and Constitutional Affairs Legislation Committee on 22 November 2024 in relation to the Privacy and Other Legislation Amendment Bill 2024 [Provisions] **(the Bill)** inquiry.

A question from Senator Scarr that was taken on notice by Ai Group and our response is set out below:

Senator SCARR: Can I ask you to take on notice—it is an important question for all stakeholders—the extent to which there was engagement with the Australian Law Reform Commission in relation to this specific concern about employee records? Obviously, organisations have workplace health and safety obligations; there are issues around alleged sexual harassment investigations. There are all sorts of issues in the context of employee records. I would be very interested to know if the Ai Group made submissions to the Australian Law Reform Commission in relation to the application of a statutory tort specifically to employee records.

Ai Group has consistently engaged with the Australian Law Reform Commission over the years in relation to its privacy inquiries where it has sought input from industry, including on the importance of retaining the employee records exemption. See for example: For Your Information: Australian Privacy Law and Practice (ALRC Report 108).

With the increasing prevalence of technology in the workplace over the past 5 years, Ai Group has specifically engaged with the Attorney-General on the need for an employee records exemption to apply to the proposed statutory tort for serious invasions of privacy – see our submission to this inquiry, including Appendices A, B and C.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

A second question from Senator Carr that was taken on notice by Ai Group and our response is set out below:

Senator SCARR: I understand that. That's neat, but we're not there yet. What are the specific concerns that would apply, if we went down this track and didn't have an appropriate exemption for employee records? I understand the coherence point. I'm trying to get to the nuts and bolts, the practical implications, that will arise if we don't have a carve-out for employee records. Feel free to take it on notice. I understand it is an abbreviated amount of time, but other stakeholders who have made submissions to this inquiry—for example, media organisations—have given specific case studies with respect to their specific concerns about how this could impact upon the members that they represent. Ms McGrath: We will take up that invitation, Senator, and provide specific case studies on notice.

Case study 1

A PCBU runs a commercial transport business and has a fleet of large semi-trailers through which it transports goods interstate.

To ensure the safety of its drivers and other road users, the PCBU implements a real-time monitoring system. The system uses artificial intelligence to analyse the driver's behaviour, looking for signs of fatigue, distraction or any type of visual impairment (e.g., if the person is eating or drinking or is using their mobile phone). It uses face tracking, head tracking and eye tracking technology via the use of cameras placed in the driver's cabin to conduct this analysis.

One driver files an application alleging the PCBU has caused them distress and harmed their dignity by monitoring them in such an intensive way – they say they are a good driver with an unblemished record and that this is an insult. They seek an injunction to stop the monitoring and the use of the software.

Parties in the "chain of responsibility" have a duty under the Heavy Vehicle National Law to minimise the risk of their transport activities, so far as is reasonably practicable This application would directly interfere with the chain of responsibility parties' ability to use safety technology to eliminate the risks of injury and harm to drivers and other road users in instances of driver distraction or fatigue.

In Europe certain driver monitoring systems are mandatory through the EU General Safety Regulation (Regulation (EU) 2019/2144)[1]. The regulations are aimed at reducing the number of accidents between trucks and vulnerable road users. For example, new trucks as of 7 July 2024 must have the following:

- Alcohol interlock installation facilitation: The rule change requires a standardised interface for alcoholic interlocks (breathalysers) in vehicles.

[1] https://eur-lex.europa.eu/eli/reg/2019/2144/2024-07-07 (4 November 2024). See also this factsheet: European Commission – New rules on vehicle safety and automated mobility.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

- Drowsiness and attention detection: Safety systems to assess the driver's alertness that for instance monitor how long somebody has been driving and warn the driver to take a break when needed.
- Intelligent speed assistance: A system that actively monitors speed and alerts the drivers if he/she is breaking the speed limit, to encourage them to slow down.
- Moving off information system: A system that warns the driver of vulnerable road users in front of the vehicle before driving off or when driving slowly.
- It is expected that further safety features will be required in the next five years, including:
- Distraction recognition and prevention: A safety warning system capable of recognising the level of attention a driver is paying to a situation and warning the driver, if necessary. This may roll out in a later phase in 2026.
- Improved direct vision from driver's position: Specific requirements to improve "direct vision" (what drivers can see directly through the windows of their vehicle) and remove blind spots. The new standards aim to allow drivers to see cyclists and pedestrians faster and easier. This may roll out in a later phase in 2029.
- Event (accident) data recorder: A "black box" accident data recorder. This may roll out in a later phase in 2029.

Case study 2

A PCBU uses cameras and sensors encrypted with AI algorithms track and analyse the actions of workers to identify unsafe behaviours, such as improper equipment handling, non-ergonomic postures, bullying/violence or harassment or any failures to follow safety protocols. When unsafe behaviours are detected, the system notifies supervisors and/or provides real-time feedback to workers. The information is also utilised to identify whether work or system design changes are needed to minimise risk and reduce reliance on people doing the right thing.

One worker has received feedback on several occasions. They have alleged that the constant monitoring and feedback causes them distress and harms their dignity. They tell the PCBU that they do not want to be monitored, as it is humiliating and degrading. The PCBU says the monitoring will continue as it is part of its risk management framework to ensure health and safety in the workplace, and is used to inform the priority for higher order controls. The worker files an application alleging that the PCBU has misused their information and intruded upon their privacy. They seek damages for their emotional distress and an injunction (interim and final) to stop the monitoring and use of the information.

This application would directly interfere with the PCBU's ability to ensure the health and safety of its workers and others in the workplace as required under work health and safety laws.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

Case study 3

A PCBU monitors how workers communicate using its IT systems, including through emails, messaging applications and virtual meetings. An AI tool analyses the data to predict and identify where and in what circumstances there may be risks of sexual or gender-based harassment, a hostile work environment on the ground of sex or other unlawful or unsafe behaviours.

One worker files an application alleging the PCBU has caused them distress and harmed their dignity by misusing information that relates to them. They have often shared private information with another worker with whom they were in an intimate relationship and the AI tool has flagged their communications as being a risk for unlawful and unsafe behaviours. The worker seeks damages for emotional distress, an injunction (interim and final) and a public apology on the basis that this harms their dignity and causes offence and distress.

This application would directly interfere with the PCBU's measures to prevent unlawful behaviour in its workplace, including as required under *the Sex Discrimination Act 1984* (Cth) and under work health and safety laws. In paragraph 9 of our submission we noted in particular the research report by ANROWS - Workplace technology-facilitated sexual harassment: Perpetration, responses and prevention, which recommends that monitoring of technology may be an appropriate prevention measure.

Case study 4

A PCBU is managing a largely remote workforce and uses remote worker monitoring software to make sure that work intensity is safe and productive in a worker's home. The software has GPS tracking, and it monitors what and where activities are undertaken, applications the worker uses and websites accessed on the PCBU-provided computer and mobile phone. It takes periodic screenshots. It alerts supervisors and the worker if they are working beyond working hours and/or if breaks are not taken as a measure to manage fatigue.

Several screenshots of a worker were recorded which required management intervention as the worker was accessing pornographic websites with a work computer and during work hours. The worker files an application alleging that this has intruded on their privacy and their information has been misused – they were entitled to be looking at any website they wanted to when they were having a break from work. The worker seeks damages for emotional distress and an injunction (interim and final) against any further monitoring while they are working from home.

This application would directly interfere with the PCBU's legislative obligations under the *Sex Discrimination Act 1984* (Cth) and work health and safety laws to prevent unsafe or unlawful behaviour in the workplace. At a fundamental level it also inappropriately interferes with an employer's legitimate right to manage their relationship with workers, including to monitor and manage workers' conduct and performance.

The Australian Industry Group
51 Walker Street
North Sydney NSW 2060
Australia
ABN 76 369 958 788

Application of exemption in these circumstances

We have already submitted that the employee records exemption in the Privacy Act should be also applied in respect of the statutory tort for serious invasions of privacy. This continues to be our view.

However, we acknowledge that the statutory tort applies to not only a misuse of information but also an interference in a person's seclusion. On that basis, if the Committee does not support the insertion of the employee records exemption, an alternative approach may be to include an adapted exemption in relation to the statutory tort for serious invasions of privacy which exempts:

> "*Activities or dealings that are reasonably necessary for a PCBU to manage or assess workers in the workplace*"

We submit that this exemption should be ongoing.

We trust this assists the Committee.

Yours sincerely

Brent Ferguson
Head of National Workplace Relations Policy

Yoness Blackmore
Principal Advisor – Workplace Relations Policy