

**Submission  
No 36**

## **INQUIRY INTO WORKPLACE SURVEILLANCE**

**Organisation:** Building Industry Group (BIG) of Unions

**Date Received:** 1 August 2024

Alison Marchant MLA  
Chair  
Economics and Infrastructure Committee  
Parliament of Victoria  
Melbourne VIC 3002



Via: [eic.assembly@parliament.vic.gov.au](mailto:eic.assembly@parliament.vic.gov.au)

Dear Chair,

**RE: INQUIRY INTO WORKPLACE SURVEILLANCE**

On behalf of the Building Industry Group (BIG) of union, comprised of the Electrical Trades Union (ETU), Plumbing Piping Trade Employees Union (PPTUEU), Australian Manufacturing Workers Union (AMWU) and the Construction Forestry Maritime Employees Union (CFMEU), we thank you for the opportunity to make a submission to this important inquiry into workplace surveillance.

BIG union members report being subjected to workplace surveillance on building sites and in their workplaces. Our unions have been consistent in opposing surveillance in all its forms, and we reject any implicit assumption or explicit statement that workplace surveillance is necessary and/or inevitable. Union members report that surveillance is far from being a niche issue: its use has become increasingly common and widely utilised, with employers tracking and collecting large swathes of data about union members. On building and construction sites, this surveillance takes many forms including:

- Use of CCTV and AI to track workers across sites;
- Monitoring the whereabouts of workers and tracking rest breaks;
- Collecting unnecessary and invasive biometric, psychological or behaviour testing as a condition of work;
- Location tracking for off-site contractors and other mobile workers, especially tracking of workplace vehicles; and
- Social media monitoring.

BIG Unions call on the Victorian Government to take urgent action to prohibit workplace surveillance in all forms as the basis of governing regulation of this practice and the technologies which are utilised to facilitate it. This submission should be read in conjunction with the Victorian Trades Hall Council (VTHC)'s submission, and BIG Unions fully endorse VTHC's recommendations as the most effective way to address workplace surveillance. The VTHC submission draws on their recent survey of Victorian workers, and union members, who have experience with workplace surveillance. Approximately 15% of VTHC survey respondents work in the industries covered by the BIG unions, and this submission will focus on the experience of workers in these industries. Crucially, over 60% reported experiences of workplace surveillance, with a further 11% saying they were unsure if their employer was conducting surveillance at work.

The most common form of surveillance reported by workers across the building industry was use of video surveillance in the workplace, being reported by 50% of respondents. The next most common forms of surveillance were email tracking (40%), surveillance on entry to the workplace (32%), and vehicle tracking (16%). Additional areas of concern included phone tracking, being

photographed without consent, having all files accessed on work devices tracked, and phones being 'tapped' to record conversations.

The use of technology on construction sites extends well beyond the often reported justification of 'monitoring for occupational health and safety (OHS)', with more than half of respondents reporting that the existence of workplace surveillance made them feel 'pressure to work harder', and a further 13.5% reported that they were certain surveillance was being used as a coercive productivity measure.

### **Case Study 1: Use of cameras**

In 2024, ETU members in construction were engaged to work onsite by a prime builder to install wiring and fixtures at the construction site for a data centre in Truganina. While working on the \$1.1bn project, members noticed numerous cameras situated around the construction site, which had been installed and used without notification or consent from the workers and their union, and had covered the bulk of the site. In June of 2024, an electrician received a written warning for breaking OHS protocol, providing a photo drawn from the cameras as evidence.

In June of 2024, the elected health and safety representative (HSR) sent a formal request for information, seeking information about whether the cameras were on, if they were recording, and their purpose. The company responded by saying the cameras were time lapse cameras that took photos every 5 minutes. The union doubted the likelihood that the photo had occurred precisely at the moment the worker made a mistake. The company assured them that this was purely coincidental.

A fortnight later a plumber on the site received a written warning, accompanied by another photo from the cameras. The union dispatched the state OHS officer and a local organiser to seek a follow up with the company to discuss the issue. Following the meeting and subsequent investigation conducted by the union, it was revealed that not only were the cameras continuously rolling, but the builder had provided a link to the direct feed of the footage for all subcontractors employers workers engaged on site, allowing them to monitor workers remotely without prior knowledge or consent.

The ETU issued a provisional improvement notice (PIN) to request the cameras be covered up onsite, and that a stop work would be issued if the issue was not addressed within 24 hours. Fortunately, the legal powers of the HSR, combined with the industrial power of the union were sufficient to enforce compliance by the company, however the threat of the company implementing new technology without consultation remains high. Further, this isolated incident is representative of a growing trend across the industry, with dozens of near identical examples being reported by construction organisers.

Further, union organisers report numerous consequences of employers' largely unrestricted right to conduct surveillance on members' OHS: High levels of surveillance at work can exacerbate hazards such as poor workplace relationships and lead to psychosocial injuries caused by little control over work and feelings of being undervalued, policed, and lacking in autonomy;

Surveillance can also discourage, and in some cases penalise, the taking of breaks, like the use of the bathroom or speaking to co-workers; and it can enforce a faster work pace and reduce downtime, increasing the risk of physical injuries.

These experiences are deeply concerning, and are the key reasons why workplace surveillance must be seen as a significant risk to Victoria's OHS laws and regulations, in addition to the risk it poses to working conditions.

### **Case Study 2: Biometric Scanning to Clock in and Out**

A company, at a regional decorating plant implemented a system from January 2024 which purported to submit workers' biometric scanning of their faces to clock in and out of work each shift, instead of the usual paper process. The company claimed that this new system was necessary because of concerns about the spread of diseases and illnesses. The new system was owned and operated by a third party.

Initially, workers were not given a choice about whether they consented to use the new system and/or provide their information to the third party. Several employees complained to the AMWU that they were worried about the security of their personal information, especially in light of the then highly-publicised leak of customer information at Optus. On behalf of its members, the AMWU applied to the Fair Work Commission for resolution of a dispute arising under the enterprise agreement (relating to a failure to comply with consultation obligations) and filed a complaint with the Privacy Commissioner under the *Privacy Act 1988* (Cth).

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

The latter is an example of deficiencies in the Commonwealth laws purporting to protect workers' privacy. Unlike an application for resolution of a dispute in the Fair Work Commission, the Privacy Commissioner appears to require individual employees to identify themselves before taking on a complaint. This clearly would have the undesirable affect of discouraging complaints by workers afraid of retaliation by their employers.

### **Case study 3: Facial Recognition**

During the COVID-19 pandemic, and the associated lockdowns experienced by Victorians across 2020-21, construction was classified as an essential service and allowed to operate under certain conditions. Using this conditionality, multiple prime builders implemented the 'simple gate system', a facial recognition software that utilises AI to track individuals onsite. At the time that it was introduced, the ETU raised the issue with various companies, however decided not to proceed with further action as they did not want to risk the operation of the industry in a time of crisis and were given assurances by the company that the system would be phased out after the pandemic ended.

However, in mid-2023 delegates on a major construction project raised the use of the system as an OH&S issue lacking in consultation. When the company failed to act, the union requested information as to the storage location and condition of the data collected by the system, but were told that the data was handled by a 'third party', and no further information was given. With the support of the union, the elected HSR issued a PIN regarding the use of the system and notified the company that a stop work would be issued if the problem was not rectified within 24 hours. Again, the powers guaranteed under the Act were effective in solving the problem, but the union has seen repeated attempts to implement alternative data collection and surveillance methods.

Another recurrent theme was the use of data collected through surveillance as evidence in disciplinary processes:

*"When I have been called into disciplinary meetings, the tracking of my movements by surveillance have been documented and used as evidence to possible termination."*

*"We had a log in log out system on our phones and if it didn't work you got a call from boss and I'm sure it was collected for later use."*

#### **Case study 4: Unreasonable Requests for sensitive information**

A company operating a note printing business with workers in Craigieburn purports to require its employees to disclose significant personal information (including health information) and the information of their domestic partners to a third party every five years. The types of information requested by the company include: a full birth certificate, all passports in the previous 10 years, a photograph of the employee, character references, names of family members and their birth dates, the employee's nationality and that of their family members, the name of any clubs, associations or interests groups of which they are a member, and their criminal history.

The company claims that this information is necessary for products it provides to overseas clients. However, it is understood that the company no longer performs that work. Further, while employees' contracts appear to require them to agree to undergo 'police criminal records' checks, it says nothing of the extensive requests for the types of information outlined above.

Several members of the AMWU complained to the AMWU that they were worried about the security of their personal information and also uncomfortable with providing the breadth of information (personal to them and their family members), especially to third parties and, apparently, an overseas recipient. On behalf of those members, the AMWU wrote to the company outlining its concerns in relation to the *Privacy Act 1988* (Cth). The matter remains unresolved and subject to discussions between the parties.

*"Vehicle tracking device used in disciplinary actions against individuals - [I knew of] at least one incident [in my workplace where this occurred] ..."*

*"Certain employees are asked to explain themselves for not completing all surveys on their service reports/tickets. Some surveys are difficult to complete due to the nature of the customer's premises."*

*"I started on the site at roughly the halfway mark of the handover date.. I became suspicious when my phone was performing differently. I later learned that the authenticator app I had been told to download was actually linked to [a company that shares the headquarters with my employer]"*

*"Vehicles have dash cams, have to continuously watch what I say & how I drive on the work site. Workshop has cameras, so have to be careful to meticulously follow the workplace rules."*

### **Case study 5: Tracking workers location**

Members at a beverage manufacturer are subject to GPS tracking in their work vehicles, which they are entitled to use for reasonable personal use.

At a vehicle repair service, members in patrol vans are entitled to take their work vehicles home. These vehicles are fitted with GPS tracking devices. Members are not permitted to disconnect those devices when not on the job. Members are concerned that their movements are being recorded even when they are not at work, and are concerned about how their data is stored and with whom.

Members at both these employers perform service work at customer locations and use work vehicles which are fitted with GPS tracking devices. They are not permitted to turn these devices off.

A flow on effect from this codified level of surveillance for the purpose of control is the reported lack of trust that employer have for their workforce, and the considerable OHS implications of this demotivation:

*"I suspect there is some kind of tracking software on the laptop I use to work from home. This makes me feel like I need to be online all the time to justify myself and guilty if I don't have anything to do."*

*"It's like living in a fish bowl. I no longer use any initiative as it may be criticised by remote viewing psychopaths."*

*"It makes you feel like uncomfortable and takes away your dignity and rights to privacy."*

*"It is intrusive, insecure, morale deflating, counterproductive and displays absolute disregard of the integrity of workers"*

*"It makes me a little paranoid like big brother is watching"*

*"Yes.. I am very nervous"*

*"Added psychological stressors"*

*"Trust deficits erode the relationship and productivity."*

*"Give your employees their right to privacy in their work space"*

### **Case study 6: Realtime tracking and shaming to modify behaviour**

Members were subject to surveillance while working, where the time by which they took to complete tasks was monitored and displayed on screens in the workplace. All passersby were able to see how long employees were taking to complete tasks.

Members complained about their health and wellbeing, including that they felt shamed into completing work at an unsafe pace, they felt it would open them to bullying or targeting by other employees, and that the practice might reduce the quality of their work.

There is considerable concern surrounding data storage and the security of third-party actors in the digital supply chain. In almost all of the case studies provided within this submission, when BIG unions requested information from employers regarding the location and security of workers' data, employers reported that it was stored by third parties who they would not disclose for security reasons. At a time when numerous data breaches are being enacted, an opaque system of security is unacceptable, especially when it concerns sensitive data collected through workplace surveillance.

### **Case study 7: Online data collection**

In July 2023, following the issues raised relating to facial recognition software across the industry, ETU members reported additional instances of surveillance and data collection. In particular, the use of an induction system, a third-party online portal increasingly used by prime builders seeking to outsource services. This system requires numerous and myriad personal data to be uploaded, even by electrical subcontractors visiting building sites. Required uploads include photos, license numbers, next of kin and other personal demographic data, most of which is used for proof of identity in a range of public and private settings. This represents a significant security risk regarding identity theft.

Further, ETU members engaged by a large subcontractor on a data centre construction site were required by the prime builder to download an app on their personal devices, a proprietary app which would track their movements about site and upload the data to an unknown location. The HSR and union representatives raised the issue and again threatened to implement a stop work condition if the requirements were not dropped, and were again successful.

The pattern of behaviour across the industry has become a case of 'asking for forgiveness rather than permission' when it comes to workplace surveillance and data collection. Without adequate

There is a substantial legislative gap through which employers conduct this extensive and excessive surveillance. However, in lieu of adequate regulation, BIG unions have negotiated to address these issues through enterprise bargained agreements. For example, the ETU negotiated a clause for inclusion in the *ETU Contracting Union Agreement 2021-2025* [Section 4.15] which rejects the implicit need for surveillance and requires the potential implementation of any tracking device or technology to be subject to numerous conditions, such as:



- Workers' inherent right to access data about them;
- Data security access and processes;
- Devices collecting data cannot do so after work, and workers have the right to turn devices off;
- Data must not be created relating to leave; and
- An employer cannot use data subject to the subject to the clause for disciplinary actions or to assess performance.

However, while unions will always fight to protect the rights and interests of workers through the process of industrial relations, the government has a moral responsibility to act when legislation does not keep pace with technological change - especially when that discrepancy allows for exploitation and excessive surveillance.

That is why we are calling on the Government to act in the interests of Victorian workers and engage in bold reforms which protect their right to privacy, safety and security.

As such, the BIG Unions endorse all the recommendations provided in the VTHC submission to this inquiry. We emphasise the urgent need to take action and call on the government to introduce a new standalone act to protect workers' privacy at work.

This new Act, the *Privacy in Working Life Act* (PIWLA) should:

1. Prohibit workplace surveillance by employers. This prohibition should apply to optical, audio, location tracking, data surveillance and biometric scans.
2. There must be a specific, non-negotiable prohibition of areas used by workers for personal use such as toilets and lunchrooms, and a non-negotiable ban on surveillance outside of work.
3. Stronger and more genuine consultation rights for surveillance should be embedded in the PIWLA, including:
  - a. Obligations on employers to demonstrate genuine need for protecting property (not for tracking workers)
  - b. Providing 14 days written notice for the introduction of surveillance,
  - c. Meaningful consultation,
  - d. Inform new employees of any surveillance in place.
4. Data security and protection processes must be further embedded, and workers must have the right to access any data about them at any time.
5. A new PIWLA must also enshrine a right to protection from adverse action or disciplinary action relating to data gained from surveillance.
6. There must be a ban on the disclosure or on-selling of data generated by surveillance to third parties - with the exception of where it is necessary for law enforcement agencies.

Additionally, workplace surveillance must be specifically scoped in to fall under OHS powers. BIG unions make the following OHS recommendations:

7. New psycho-social health regulations specifically apply to the risks generated by workplace surveillance.
8. A workplace surveillance guide be produced by WorkSafe (in consultation with VTHC and unions) about how to address workplace surveillance.

Workplace surveillance provisions must be enforceable. BIG unions make the following enforcement recommendations:

9. Fines be issued against employers who breach obligations imposed under a new PIWLA.
10. Civil remedies be available to individual workers (or groups of workers) who have suffered loss due to wrongful workplace surveillance.
11. Unions and the Wage Inspectorate Victoria have powers of investigation and to launch enforcement proceedings before the Court.

Thank you again for the opportunity to make a submission into this important inquiry. Should you have any further questions please do not hesitate to contact Tiarne Crowther at the VTHC on [REDACTED]

Kind regards,  
[REDACTED]

Luke Hilakari  
President Building Industry Group  
On behalf of Building Industry Group of Unions

