T R A N S C R I P T

LEGISLATIVE ASSEMBLY ECONOMY AND INFRASTRUCTURE COMMITTEE

Inquiry into workplace surveillance

Melbourne – Tuesday 3 September 2024

MEMBERS

Alison Marchant – Chair
Kim O'Keeffe – Deputy Chair
Anthony Cianflone
Wayne Farnham
John Mullahy
Dylan Wight
Jess Wilson

WITNESS

Kat Eather, General Counsel, Business Council of Australia.

The CHAIR: Welcome to the public hearing for the Legislative Assembly Economy and Infrastructure Committee's Inquiry into Workplace Surveillance. All mobile telephones should now be turned to silent.

All evidence given today is being recorded by Hansard and broadcast live on the Parliament's website. While all evidence taken by the Committee is protected by parliamentary privilege, comments repeated outside this hearing, including on social media, may not be protected by this privilege.

Witnesses will be provided with a proof version of the transcript to check. Verified transcripts and other documents provided to the Committee during the hearing will be published on the Committee's website.

Thank you so much for your time today. I will do a quick introduction of everyone, then I will pass to you to maybe make some opening remarks and then we will head to some questions.

Kat EATHER: Sure thing.

The CHAIR: So thank you. I am Alison, Member for Bellarine.

Kim O'KEEFFE: Hi, Kat. I am Kim, Member for Shepparton.

Anthony CIANFLONE: I am Anthony Cianflone, Member for Pascoe Vale.

John MULLAHY: John Mullahy, Member for Glen Waverley.

Dylan WIGHT: Dylan Wight, Member for Tarneit.

The CHAIR: I might hand over to you if you would like to talk a little bit or give an opening statement. It might help us kick off with some questions.

Kat EATHER: Sure. I am Kat Eather. I am the General Counsel, and I also look after workplace relations policy, for the Business Council of Australia.

Thank you for the opportunity to appear before this committee today to talk about workplace surveillance. Coupled with the benefits to safety and compliance that can be generated by technology with surveillance capacity, Australian employers and workplaces are subject to a comprehensive framework of legislation and regulation that touches on almost every aspect of the way that we work. Many of these laws already regulate aspects of workplace surveillance or how records of surveillance may be used in relation to employment or otherwise provide a basis for why workplace surveillance may be required to ensure compliance and keep employees safe at work.

While Victoria does not have a standalone law dealing with workplace surveillance, existing Commonwealth and state laws that deal with aspects or effects of workplace surveillance include the Occupational Health and Safety Act, the Fair Work Act, the Privacy Act and the *Surveillance Devices Act 1999* (Victoria). In addition to this, both New South Wales and the ACT have targeted workplace surveillance legislation which requires employers to provide employees with notice of workplace surveillance and have appropriate workplace policies in place. In the BCA's experience, it is generally considered best practice, and indeed the actual practice for employers operating outside of those jurisdictions, to adopt similar notification of surveillance requirements as those imposed in New South Wales and the ACT—that is, employers will implement a standard policy and notification process for their business which is at least compliant with the minimum standard requirements in New South Wales and the ACT. They do not have separate approaches in different states.

A transparent approach to workplace surveillance is not just desirable but necessary. It aligns with the approach of industrial tribunals such as the Fair Work Commission when determining the fairness of discipline and dismissal of an employee due to conduct detected on an employer's computer systems or other surveillance devices. The ability to monitor workplaces and interrogate actions that have occurred on an employer's technology or communication system and devices can be critical for a range of reasons, ranging from worker safety to security of equipment and premises, recording working hours and attendance to ensure wage compliance and that adequate breaks are taken, and that employees are paid properly. It is essential that any move to further regulate workplace surveillance in Victoria does not impede the use of surveillance for those essential functions.

BCA members use technology capable of workplace surveillance such as CCTV cameras patrolling construction sites to identify areas of work such as pipes that need to be checked. Developments in construction also include the use of wearables to keep workers safe, such as vests that allow automatic avoidance of machinery and helmets capable of monitoring heat stress. AI-led monitoring of customer call centres in real time is leading to tangible improvements for employees by identifying abusive content as it happens. BCA members can provide immediate support to their team and lower risks of psychosocial hazards and burnout.

As covered in our brief written submission, there are a number of inquiries, reviews and anticipated changes to legislation on foot already which will touch on or affect aspects of workplace surveillance in Victoria. In particular amendments accepted either in full or in principle by the Commonwealth government arising from its review of the *Privacy Act 1988* include enhanced privacy protections for employee records, regulation of geolocation tracking data and broader changes to the rules for the collection, storage and use of personal data. The Commonwealth House of Representatives Standing Committee on Employment, Education and Training is also examining the issue of workplace surveillance as part of its inquiry into the digital transformation of workplaces. The BCA's view is that this inquiry should consider the outcomes of those processes before assessing the potential need for further regulation of workplace surveillance in Victoria. Further data is also required about the prevalence and impact of workplace surveillance before the need for further regulation can be properly assessed. Thank you.

The CHAIR: Thank you so much, Kat. We will head to some questions, and we might start with you, Kim.

Kim O'KEEFFE: Thank you. You did actually raise the Commonwealth having that inquiry looking into workplace surveillance, but our understanding is that the Privacy Act and the proposed reforms do not specifically cover workplace surveillance in that inquiry. Why should Victoria hold off on considering law reform in this space? We do not know how long that is going to take, why should we hold off?

Kat EATHER: My understanding is that we will expect some of those reforms imminently. The Attorney-General has said that they are working on that and hoping to introduce legislation by the end of this year. The BCA would obviously love to see an exposure draft, given the extremely wideranging impacts that the Privacy Act reforms are likely to have.

While it might not deal potentially with workplace surveillance specifically, to the extent that amendments are made to the employee records exemption I think that will have a real impact on the records produced by workplace surveillance. I think they are also looking at defining geolocation tracking and further tightening up biometric data, which will also have an impact, I think, on surveillance, which is used very broadly in a range of the submissions here from biometric time and attendance systems through to trackables. Certainly the data produced by a range of that technology will likely be impacted by the Privacy Act reforms. I think the small business exemption, which I heard mentioned earlier, is also under review, subject to further consultation. So there is the impact for a lot of the concerns that are raised in this inquiry about the handling of data, about the handling of employee records and about the exemption of small business to be dealt with subject to the amendment Bill that is released by the Commonwealth government.

Kim O'KEEFFE: Thank you.

Anthony CIANFLONE: Thank you. Thank you for appearing. We heard earlier from the Office of the Victorian Information Commissioner on privacy—just some of their insights into and experiences of how businesses store and retain or delete or do not delete relevant data as time goes on. In your experience and with that in mind, how extensive would you say workplace surveillance is amongst your 130-odd members and businesses? They actually represent 250,000 workers in Victoria, which is huge. What benefits do they gain from it, would you say? And how, as far as you are aware, is that data appropriately managed, stored and then deleted when it is no longer needed?

Kat EATHER: That is a big question. How is it used? I think in a variety of ways. And a lot of the time surveillance is necessary, not for, necessarily, productivity or employee management but for compliance—for employers to comply with a range of other laws that they have. One of those is time and attendance. In order to comply with the various kind of awards and enterprise agreements that cover our members, employers need pretty detailed records of when employees are working, the exact times that they are working, the times they have taken breaks, whether they have taken overtime, whether they are working at hours of the day that attract

penalty rates. And with wage theft laws due to commence in January and increasingly high civil penalties under the Fair Work Act under the closing loopholes reforms, it is essential that employers have accurate records of that.

Safety is another really important reason. We are seeing workplace surveillance lead to increasing ways to keep employees out of harm's way, whether that is, I guess, camera-led vehicles in mines, cameras that can go down pipes or drones that can fly above vats of dangerous chemicals where you used to have to send employees up stairs in bad weather to have a look. Things that can be done using CCTV or camera technology so that you do not need to send physical people into high-risk environments I think is another way that surveillance technology is improving the way that people work and is benefiting employers.

In terms of data storage, most if not all of the BCA's members will be covered by the Commonwealth *Privacy Act* at an absolute minimum, and I am hearing that some of them may be covered by Victorian privacy legislation to the extent that they have Victorian contracts as well. That will regulate a lot of how records are stored. Employers also need to keep various employee time and wage records under the *Fair Work Act*, and so the outcomes of some of those surveillance technologies—for example, time and attendance records systems—need to be stored in compliance with the *Fair Work Act* and those records need to be able to be produced to employees or ombudsman inspectors on request. I could not be more specific than that, given the diversity of our membership.

The CHAIR: John.

John MULLAHY: A lot of your members are obviously working across borders. New South Wales and the ACT have specific workplace surveillance laws. How workable are these laws for your members in New South Wales and the ACT, and could they be improved in any way?

Kat EATHER: I think they are workable. In New South Wales we have had the Workplace Surveillance Act in place since 2005, and it is broadly consistent with the ACT legislation, so I think they are manageable. Consistent things that members will do to comply with those Acts are to give notice, commonly in employment contracts, because their surveillance systems will already be established by the time new employees are now starting and have comprehensive surveillance policies in place. My experience with our members and also as a private practice employment lawyer before joining the BCA is that companies that operate nationally and internationally will have a standard workplace surveillance policy that applies Australia-wide. It will not be 'Here's our New South Wales surveillance policy'. Typically you would have additional notice provisions as well—so tracking devices in vehicles will be signposted and cameras will be put in prominent locations and signposted—and commonly members logging on to computer and ICT systems will get a notification as they log on that the use of the device can be monitored by the employer, if that is the approach that they take.

John MULLAHY: So would your members then base their Australia-wide policies on New South Wales and the ACT, because that is more stringent?

Kat EATHER: Yes. It would need to be the standard to comply with the highest level of legislation required.

John MULLAHY: Yes. But could there be any improvements on that?

Kat EATHER: Some members have raised that the 14-day notice provision, which I think is consistent in both Acts, can be problematic, where an employer has not previously had workplace surveillance but then needs to interrogate their systems because a complaint has been made—for example, about sexual harassment, bullying, fraud or some other regulatory reason, and they need to go and interrogate emails that somebody has been sending or receiving on a work system. In those situations, having to give 14 days notice will often cut across the purpose of the surveillance in the first place. It would allow people to go in and delete records. It would allow them to obscure or respond to things. So that has been raised from a couple of employers with me as being problematic. Otherwise, I generally think that the notice and policy requirements are reasonable.

John MULLAHY: If there is any new surveillance, they would have to give notification and all that sort of thing. Employers that have currently been there for many years, if they make any changes to surveillance, notification, all that has to go out to all employees?

Kat EATHER: If they introduce new forms of surveillance. So if you, for example, had only had computer and email monitoring but you then wanted to introduce geolocation tracking in your vehicles—GPS tracking—or you wanted to introduce camera surveillance, then yes, you would have to update your notice and policy to comply.

John MULLAHY: Thanks.

The CHAIR: Dylan.

Dylan WIGHT: Thank you. My question is along similar lines, but I think we have just got a pretty decent overview of how the Acts work in New South Wales and the ACT. Your submission talks about if there were to be legislative change, it would be important to align with those two jurisdictions in particular given our proximity to them and businesses that work across those borders. So in both of those Acts employers have to disclose type of surveillance, when the surveillance commences, whether it is limited or ongoing surveillance and whether it is imminent or continuous. You spoke about the fact that in Victoria it is best practice for employers to do that anyway. Whilst it is best practice, in my experience, it is not always the case, and I would even go as far as saying that it is not common for employers to disclose absolutely every single piece of surveillance that they have or that they are using with respect to their employees. Would the Business Council of Australia support legislation that provides those extra safeguards to workers in Victoria, like we have in the ACT and New South Wales, given you are saying that most of your members are complying with that regardless?

Kat EATHER: I think the business council's position would be that we would still recommend that the Inquiry await outcomes of the other Commonwealth inquiries in relation to the Privacy Act and the digitalisation of the workplace first due to the wideranging complexity and huge amounts of workplace regulation legislation that members already need to deal with, particularly when they are operating across state lines and nationally. Without specific feedback from members on that point, I do not think it would be too much of a stretch for most of the BCA's members to comply with the notice and policy requirements that are in place in New South Wales and the ACT, because I would believe that most of them would already do that.

Dylan WIGHT: Just one more—is that all right? Out of the federal legislation and what we are going to see from the Inquiry that is happening federally at the moment, I do not think there is going to be the capacity, or I do not think there is going to be legislation that catches those safeguards in particular. I just do not think we are going to be in a situation where, if we were to wait or if that was the case, those inquiries are going to address those safeguards which are some of the most fundamentally important pieces of those two pieces of legislation in the ACT and New South Wales. So given that, is the business council in a position where it would support that legislative change, if we were moving towards legislative change?

Kat EATHER: I think subject to the terms of the legislative change, the BCA would accept that it is reasonable for employers to give notice to their employees about surveillance taking place. I have already said it, but I believe that most of the BCA's members, if not all of them, would do that, particularly in relation to computer and email monitoring and the signage of cameras and GPS location tracking. So I think the BCA would accept that that is a reasonable approach. I think most employers would accept that that is a reasonable approach. I know there has been a lot of talk about *Nineteen Eighty-Four* and Orwellian, dystopian kinds of workplaces, but it is my genuine belief that, at least in terms of the BCA's members, most employers want to work well with their employees. They want happy, engaged and safe workforces because that is the way that business is successful. Business does not gain a lot in the long term from having a depressed and run-down and paranoid workforce that believes every moment of their life is being tracked. I do believe that having surveillance to a level is causing psychosocial harm to your staff, that is causing undue stress and anxiety, is already a breach of employers' work health and safety obligations. In some state jurisdictions that is expressed under the kind of psychosocial code of practice. In Victoria it is clear that employers' obligations to minimise risk for the health and safety of their employees also covers psychological harm as well.

I think most employers would accept that they should not be using workplace surveillance in a way that causes harm, including psychosocial harm, to their employees, and providing notice is one way of minimising that harm as part of any normal risk mitigation strategy. It is also part of an important change management process. When they are introducing new technologies, businesses want it to be successful. They invest a lot of money in this, so part of that is bringing your staff along for the journey and making sure they understand the technology.

But ultimately if employers want to use the outcomes of workplace surveillance in terms of disciplining or ultimately dismissing employees for the productivity concerns, then they need to be transparent. If you do not have both a valid reason and a fair process in relation to a dismissal, the vast majority of your employees will have access to unfair dismissal claims in the federal jurisdiction, which covers most of our members, and failing that, there are other types of workplace claims that can be brought as well. So it is in their best interest to be transparent to the degree necessary I guess to be procedurally fair to their staff.

The CHAIR: Can I just talk about AI for a moment. It seems to be coming up and it is some technology that we may not even be aware of yet or will be coming in the coming years. Can you give an example maybe of where you are seeing AI being used and what should we consider as a committee in legislating AI?

Kat EATHER: I think AI is being used in a range of areas, not to I guess wholesale replace jobs or people but to replace tasks. We have seen financial institutions using AI to review large-scale customer documentation, for example, with loan applications, which frees up staff to do more high-value work I guess in terms of engaging directly with customers or other employees. We see it replacing some administrative tasks for bid managers in some industries so they can focus on the actual business development. It is being used in recruitment, and there are concerns raised about that in terms of bias and discrimination but there is also opportunity there to I guess decrease bias and opportunity in the way that those systems are trained and the information that they learn on. So I think there is a huge amount of benefit and productivity benefit to be harnessed from AI. The uptake does need to be safe and responsible and principled. I am aware that there is another Commonwealth inquiry being led out of DISR looking into that, which a lot of our members are keenly and actively participating in. Sorry, I forgot the second part of your question.

The CHAIR: Just more how to legislate. Can you do it in a technology-neutral way with AI sort of coming so quickly?

Kat EATHER: With AI we do look for, I think, principles-based and technology-neutral legislation as far as possible. I think of key interest to our members in relation to artificial intelligence is that it is looked at as I guess a whole-of-government or whole-of-nation response so that we do not have piecemeal legislation popping up in all different areas that makes implementation difficult or impossible so that people will not harness the benefits—the safety and productivity—that AI can bring. It does need to be principled. I think there are already a range of protocols and principles being developed. And it needs to be internationally interoperable too so we can be cohesive with international jurisdictions and that multinational corporations and the technology that is developed overseas can be brought here in a safe and responsible way.

The CHAIR: Thank you. Kim.

Kim O'KEEFFE: Just one of our questions: what impact would more stringent workplace surveillance laws have on small businesses in Victoria?

Kat EATHER: I think with the focus of the BCA, obviously our members are not small businesses—they are large businesses—but we do work closely with COSBOA and the relationship between large and small business is essential and something that is important to us. Having worked with a range of small businesses myself, I think any additional regulation is a challenge for business. It is an added cost in times when, you know, there is an increasing number of failures with small businesses and the regulatory burden is incredibly difficult. So I think to the extent further legislation that impacts small business is introduced, clarity, simplicity, harmonisation with the existing regulatory regimes, information, guidance and support are all essential to ensuring that small business can comply without, I guess, further impost and kind of unnecessary red tape.

Anthony CIANFLONE: Just picking up on a couple of the other points from earlier on and your point around most businesses obviously, or all businesses really, not wanting to have staff working in a really high-pressure, scrutinised environment because that is not good for workforce and business outcomes of course, a lot of the data that is increasingly being held by especially bigger businesses, not so much the smaller businesses, is quite personal and sensitive in nature. Particularly with the increase in cyberattacks and malicious sort of activity online—we have had quite a few keynote and significant high-profile data breaches around Medicare and Optus, just to name a few, and some may even be your members—my interest obviously through the Inquiry is around workplace surveillance, but a lot of that data that has been accumulated and harvested within those businesses by those business managers and workers is of a consumer nature too. So through that lens, I

guess, how can we look at it from that angle, from a business point of view, through this inquiry for any potential legislation that may strengthen safeguards and provisions around consumer safety and workplace safety in tandem through any potential state legislation that complements federal and other jurisdictions as well?

Kat EATHER: I think they are really important issues, and I think most of our members would accept that the Privacy Act does need reform—certainly the cybersecurity needs to be enhanced. So I would not, I think, dispute anything that you have said there. I think cybersecurity, consumer safety and data protection are all really important and critical issues. I guess the main point that I would make there is that those are issues that are being dealt with as we speak at a Commonwealth level. To that extent my primary submission would be that we really do need to wait and see what the federal government is going to do there. I do understand that we are going to see legislation very soon. To the extent that Victoria considered that the *Privacy Act* reviews did not address all of the harms identified in that area by this inquiry, we would be looking for legislation that is consistent and harmonised and does not create additional or inconsistent burdens, because it becomes confusing, difficult to comply with and a productivity handbrake and does not tend to offer benefits for any of the stakeholders when the legislation is confused and inconsistent.

The CHAIR: We really appreciate your time today, Kat. If there is anything further or something that has been brought up today that you think you would like to add further for the Committee's consideration, you are more than welcome to add some more submission to the Committee. Thank you so much for your time, though, and answering our questions today as well.

Witness withdrew.