T R A N S C R I P T

LEGISLATIVE ASSEMBLY ECONOMY AND INFRASTRUCTURE COMMITTEE

Inquiry into workplace surveillance

East Melbourne – Thursday 26 September 2024

(via videoconference)

MEMBERS

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

WITNESSES

Scott Barklamb, Principal Advisor, Workplace Relations Policy, and

Yoness Blackmore, Principal Advisor, Workplace Relations Policy, Australian Industry Group.

The CHAIR: Welcome to the public hearings 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 of 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.

I remind members and witnesses just to mute their microphones when not speaking, to minimise interference.

Thank you very much to Scott and Yoness for joining us today. What I thought we might do is allow you to have some introductory or opening remarks. You might like to talk to your submission or just something further you would like to add, and then we will jump straight into some questions from our committee members. I will hand over to either of you.

Yoness BLACKMORE: Good morning. Thank you, Chair and members of the Committee. My name is, as you know, Yoness Blackmore. I am a Principal Advisor in the Workplace Relations Policy team at Ai Group, and I am here with Scott Barklamb, also a Principal Advisor in the same team. As we have only got 30 minutes, we will not deliver an opening statement. You have had the benefit of our submission, and you have information on Ai Group. Our submission is marked 40. With that very brief introduction, we will be pleased to take questions.

The CHAIR: Perfect. I think we probably all appreciate that because we can just jump into the nitty-gritty of it and things that the Committee members are interested in picking a bit further. Anthony, I am going to go to you first.

Anthony CIANFLONE: Thank you, Scott and Yoness, for appearing and for your very comprehensive submission as well, which I have gone through. Thank you. Look, we have heard quite a lot of evidence, especially from the employee and the union and worker representative side early on through this inquiry, basically in relation to what is really appearing to come across as a lack of awareness from the workers' perspectives about how they are being surveilled, how they are being monitored and how their data is being stored and utilised. We have not heard really of any examples through the evidence or the submissions around when an employer proactively seeks to consult with the worker in relation to how they are being monitored and to proactively seek their affirmative consent to that monitoring. I note that your submission strongly recommends that this committee awaits the federal changes being looked at through the privacy legislation that is going through their in-tray at the moment. I guess what I am getting at is how we can as a committee come into this space to make proactive recommendations and get that balance right from your perspective, an employer perspective, but also recognise that employees also have a right to be better aware and consulted about how they are being surveilled going forward, because it is an issue. It is a strong concern that I am very cognisant of and that I know many others in the Committee are cognisant of, so I am so keen to hear Ai Group's view on that

Yoness BLACKMORE:The Ai Group view is that our members make their employees aware of any monitoring, and our members do it for various reasons that are well supported. But if our members actually do want to take any action in relation to the monitoring, they will be facing difficulties—for example, with the Fair Work Commission. It is well established that there needs to be a policy in place so that employees know what they need to do in the workplace and what standards of behaviour apply. They need to understand how that monitoring is taking place, and they need to understand that there are consequences of the monitoring. So our position would be that for employers really it is in their interest to make employees aware, and that in itself is what achieves a balance.

Scott BARKLAMB: Can I just add to that second part of your question, which I would sum up, Anthony, as: how can this committee make a difference? I think we would make the point—and you have picked it up, but we would just like to stress it again—that finding that space will arise as the federal law clarifies and as various processes play out. We would encourage the Committee to have a careful think about the sequencing of

events next year and the point at which it can usefully make directed recommendations. Without conceding specifically what those recommendations might be, we really do reiterate that point about sequencing and an informed understanding of where any regulatory space may lie and then evaluating what is right, what is balanced and what is practical within that.

Anthony CIANFLONE: Thank you. I acknowledge Ai Group's position and advice to almost encourage employers to be disclosable around what and how employees are being monitored. But it does really appear generally in terms of the evidence we are receiving that a lot of that is based on a lot of goodwill and good faith, and that is the space where employees and union representatives are saying from their perspective that there is a lot that could be done to come halfway in that regard.

Scott BARKLAMB: I think that is true. Can I pick up—just quickly, Yoness, if I may. Our predecessor made some really good comments—our colleague Daniel made some good comments—clarifying the introduction of major change type provisions in awards. The significance of the change is an area that has been litigated and which ones do and do not fall within that, so that would need to be examined in regard to workplace surveillance. Yoness has already pointed to this, but this is something else I would really stress to you: an employer acting on surveillance information has a lot of controls through the Fair Work Commission processes relating to unfair dismissal in particular and also some capacities to take disputes in relation to counselling and discipline, but the veracity of the reasons for the dismissal, the procedures that are followed and the fairness of dismissal matters being put to employees—all of those are known controls on information—however it is sourced, and the surveillance information falls well within that known quantity.

Anthony CIANFLONE: I am mindful of the time and others having a go too. But thank you; that is good.

Yoness BLACKMORE: Could I add—just quickly, Anthony—I am sure that the Committee is aware of the statutory tort for a invasions of privacy that is in that first Privacy Act amendment bill. That may be of relevance here. Sorry to interrupt.

The CHAIR: Thank you for that. I will go to Kim to ask the next question. Thanks, Kim.

Kim O'KEEFFE: Sure, thank you. Thank you for your submission; it is really helpful. We have seen lots of different things coming through, and this has a different type of theme again, which is great. As a former small business owner I suppose I am very interested in your submission where it notes that the Privacy Act exempts small businesses as well as employee records. How can we ensure that exempt businesses undertaking workplace surveillance protect the privacy of their workers?

Yoness BLACKMORE: I guess the first thing to say here is that we acknowledge of course that small business exemption. This is something that is being considered directly in the review, and I am sure you are aware of that. In relation to small business we would reiterate what we have said before in answer to Anthony's question, but I would also point out again this new statutory tort that is being proposed to be implemented. It is a right for an individual to take action against any organisation, whatever size, in relation to the misuse of their information and for interferences in their seclusion. I think we are actually getting some progress at that federal level, which probably again emphasises the importance of sequencing here. But what would probably be the most helpful thing would be best practice guidelines and whatever can be produced to make it easy for small business to generally make sure that their employees are aware and they have policies in place supporting better decision-making.

Scott BARKLAMB: I will just augment that with one quick comment, Kim, and thanks for the question. Something magic does not happen once you hire your 15th employee. This is really challenging for a range of businesses right across the small and into medium-sized sector that is really important through Victoria as well. This is a challenging area. It is one more piece of complexity, regulation—one more thing that small businesses need to understand and comply with and deal with—and it needs to be understood in that context.

The CHAIR: Thanks, Kim. Dylan, I will head to you.

Dylan WIGHT: Thanks, Chair. And thanks, guys, for your submission and your evidence. Your submission talks about Victoria's Surveillance Devices Act and also the Privacy Act being adequate to regulate workplace surveillance. I guess just from my point of view I would like your response to the litany of evidence that we have had that those two Acts and the current framework that we have in Victoria are just fundamentally

inadequate to be able to deal with this—to be able to deal with it, firstly, from an employer's rights point of view, I guess. I mean, there are issues around consultation and consent that we have heard about. There are issues around data ownership and data access that we have heard about. There are issues around disciplinary procedures that we have heard about. There are just issues around collectively organising. There are issues around the sort of workplace balance or balance of power in the workplace and how surveillance is continuing to skew that in one way.

Also, I would probably make the point that, particularly for some employers—some that, frankly, may not be members of your organisation—I think there are some issues within this as well where there is just an absolute lack of understanding because there is no clear framework as to what is kosher, what is okay and what is not. I would probably suggest that there is capacity there for some employers to get into a spot of bother as well. So with the mountain of evidence that we have had in that respect, I would like your response as to the position in your submission that the current framework is adequate.

Scott BARKLAMB: I might have a first go at that, and perhaps Yoness should come in afterwards. I think a comment was made when we were listening in earlier that there are few employers that have taken part and it was a different voice in what you have heard. The preponderance of evidence might be listening to different constituencies or looking at different materials. From what we understand, employers do have a commonality of concerns that lead them to consider surveillance. Employers are widely concerned about safety; avoiding sexual harassment; having oversight of usage of vehicles, equipment, assets et cetera; and understanding conduct with customers and interactions and clients and other people in the workplace. So the driving concerns for surveillance—they are not benefits; they are demands on employers that drive this—are fairly common. In terms of the inadequacies of the law, our primary submission is that those inadequacies are met with information—that that is the best opportunity considering the context, the mix of federal and state law, and that information resources, guidance, good practices and case study examples are the best approach here. We are not clear that these are common questions in workplaces. They may be of concern to some in some contexts. They may be of increasing concern in particular industries or particular industrial profiles. I do not think we know that yet. We do not know that correlation yet to think about it. So really I think the basic point we want to raise is yes, there is an information deficit to some extent because technology has changed and demands have changed continuously on employers to need to know and manage risks, but we think the best measures do not necessarily lie in trying to carve out additional regulation at state level.

Dylan WIGHT: Can I just say the point of the Inquiry is to try and fill some of that information deficit that we have. We have heard a significant amount of evidence not just from employee representatives but also from academics and different think tanks as well that this is becoming a common concern and increasingly becoming a common concern. I will also pick up the point in respect to the weighting of opinions that we have had in this inquiry. We have actively sought to have employers come to this inquiry and present evidence, and they have not responded or they have said no. So we are working with what we are working with. I would make the absolute point from the evidence that we have heard that this is an increasing concern to a lot of workers, to academics, to think tanks and to unions, and I would think it is probably an increasing concern to your members as well. I do not accept the notion that waiting for what may come from the federal government is going to fix the inadequacy that we have in Victoria. I think that much is clear.

Scott BARKLAMB: Respectfully, you do not know the extent to which the actions at the Commonwealth level will obviate the need for action at the state level that you might find. You do not know the shape of the law in Victoria going forward because you have only got partial jurisdiction, considering the Privacy Act. So it is not necessarily a submission saying that you should not take any action as a result of your inquiry, it is a submission saying that you have got a clear known unknown in the new year and the timing and sequencing of events would best lead to an emphasis on supporting and encouraging good practice in the immediate term but in the medium term, when you do know the certainty going forwards, perhaps reopening the conversation.

Dylan WIGHT: I do not think we have got a situation where we have best practice playing out in a lot of workplaces in Victoria. But I would also make the point that the terms of reference for what the federal inquiry looks like at the moment do not and are not going to deal with a lot of this. It is not. We know the parts that it is not going to deal with already.

Yoness BLACKMORE: I wonder, Dylan, when we are talking about the Privacy Act—sometimes with surveillance, everyone talks about the monitoring, and we are all conscious of that, right? No-one wants to be

monitored all the time. But I suppose it is really about the use of the data—what is being collected but what is being used. Now, if the employee, for example, is working from home, what exactly are we talking about here? Are we talking about the use of the data primarily from the monitoring?

Dylan WIGHT: Well, I mean, I think we are talking about a whole bunch of different things. I think we are talking about the need to consult prior to introducing, which we spoke about with the VACC previously when speaking about consultation prior to introducing surveillance. We are talking about ownership of the data. We are talking about how the data is used.

Yoness BLACKMORE: Yes.

Dylan WIGHT: We are talking about a whole range of different things, I think.

Yoness BLACKMORE: The Australian Privacy Principles really are very directed to that, because we are talking in there, for example, about transparency—acknowledging of course that the small records exemption is sitting there at the moment. In terms of the government response, they have in principle suggested that there are going to be some changes there. But it is looking at transparency, so people have to know what data is being collected. In terms of collection, if the Australian Privacy Principles apply and it is sensitive information, then there needs to actually be consent. It needs to be reasonably necessary. There is the principle of not keeping information longer than necessary and only using it for the purposes that it is collected. So of course I am not in any way taking away from what you are saying and that is not the intention, but I do think the Privacy Act has a lot of work to do, especially in a context where data itself is so mobile in terms of where it goes. Is not the best place for that perhaps under the Privacy Act?

Dylan WIGHT: Yes. Look, I will let someone else ask a question, so I can just leave this as a comment. I think what you say is right, but I think it is primarily looking at data collection and data storage. It is not looking at it through in any way an industrial relations lens.

Scott BARKLAMB: No, but that is when the consultation provisions and the unfair dismissal system and capacity to raise disputes arise—and collective bargaining, potentially.

Dylan WIGHT: Yes. Like I said, I will leave it as a comment.

Scott BARKLAMB: Yes, sorry. I should have let you leave it as a comment.

The CHAIR: Thank you, Dylan. Wayne, I will go to you next.

Wayne FARNHAM: Thank you, Chair. Thank you, Scott and Yoness, for coming today. Thank you, Dylan, for chewing up all the time; that was great. I am going to go back to what Kim was talking about a little bit earlier. It was around best practice guidelines. Now, my background is I ran businesses for 30 years before I got into the job I am in now. Your submission does favour best practice guidelines over regulation. My initial thought is guidelines can always be open to interpretation whereas regulation is more clearly defined. Why do you think guidelines are better? I have probably got the opposite view, even coming from private business.

Scott BARKLAMB: Yoness, would you like me to open on that one? Regulation is generally, with the exception of small business differentiated regulation, expressed generically as requirements. Guidelines can speak to a range of different circumstances: small, medium, large, unionised, ununionised, existing consultative mechanisms, informal consultative mechanisms et cetera. So guidelines, in our view, can speak to more circumstances more flexibly and encourage good and open practice. If you have a regulation that says 'Do A, B and C', the unfortunate reality of our industrial relations system is people will do A, B and C only and you will have a dispute about whether you have done A, B and C, rather than thinking through 'Have I best had a dialogue with my people? Do they understand why I am doing this, why I am introducing this form of surveillance? Do they understand why I am updating the surveillance?' An example that I have come across recently is someone had four brand new utes stolen from their business. There is a reason they are putting in tracking technology now—distinct from real-time tracking of location, just theft tracking. You can have that dialogue. You can have that open communication. Now, in some workplaces that communication will be industrial in nature or it will take advantage of the union presence in the workplace, or it will be more oppositional in the context of other blues that people might be having. Yes, we think guidelines are more flexible to more circumstances and more nimble to the changing legal situation that Yoness has spoken about,

the known unknowns of what is happening in the wider regulation, recalling that in Victoria we are not sovereign on our workplace regulation. Much of it is coming from the federal system and the federal Parliament, and that is just the reality that we have to work with.

Yoness BLACKMORE: I might add to that as well one of the advantages of course of having the guidelines is you can look across the spectrum of regulations that do apply within that worker relationship. Obviously you have got your work health and safety and there are a lot of positive things that come out of surveillance in that respect. We have positive duties in terms of sexual and gender-based harassment where technology can be used to perpetrate sexual harassment, and there has been a recent report, which I am happy to share with the Committee from ANROWS, actually recommending monitoring in that context to try and prevent those behaviours. There are a number of examples that I can give here, but guidelines have the advantage, particularly for small or medium businesses, to help them look across all these different laws and regulations that apply to the employment relationship and then to make sure that the monitoring they are doing in that cross-purpose way is brought together.

Wayne FARNHAM: Thank you. I will let someone else have a go.

The CHAIR: Thank you, Wayne. I will go to John, thank you.

John MULLAHY: Thanks, Chair, and thanks, Yoness and Scott, for being here today. I will just pick up on your submission that the Privacy Act and the Surveillance Devices Act are adequately regulating workplace surveillance. However, we have seen that New South Wales and the ACT have already enacted workplace surveillance laws. Using New South Wales and ACT as an example, how do your members find the application of these laws, and could they be improved in any way? Do they have any recommendations that we would bring back from this committee?

Yoness BLACKMORE: Thank you, John. I think it is difficult to say from member to member how they are coping with these things on the ground, but obviously there is a regulatory and administrative burden for our members. I probably could not really go there on that legislation other than to say of course that it supports awareness, which we have already said is what employers need to do in the workplace. If you are asking if these sets of legislation may be applied in the Victorian context, I think it is difficult to determine that. As we have put in our submission, it is our view that the Surveillance Devices Act does a good job. There is this sequential review of the Privacy Act that will then address the data issue, which is of prime concern within this inquiry, and that would be our submission on that. Scott, did you have anything else to say?

Scott BARKLAMB: Only that I believe there have again been some reviews across the past two years in New South Wales of the state legislation, so again we have got a little bit of uncertainty about quite where the future approach is sitting. Even were you—and I only do this for the sake of argument—to try and pursue congruence with New South Wales, we are not clear what the New South Wales approach will be going forward for too long. There is a New South Wales and an ACT model, sure, but there is also Queensland, Victoria, WA, Tasmania, South Australia and the Northern Territory, who are pursuing a very different approach, and that should not be dismissed. The only other thing I would say is—and I raise this just from examples in other areas of the law—were any attempted comity or consistency to be pursued, be very cautious about taking a different approach to penalties and liabilities. Comity is comity, it is not pick and choose how you would like to apply those things. Now, we would want to be heard on any proposition to try and pick up laws in a different state, were that is a direction that was pursued. But just that caution—we occasionally see states say that they are making a law consistent with approaches in other states and in reality, once you look at the detail, that is not actually the case.

John MULLAHY: So take no action and wait until the federal government does, but try and harmonise across jurisdictions, or not?

Scott BARKLAMB: No. Our general submission is that a great deal can be achieved with information and encouragement—and if we do not say this in our submission, we should—and that should be developed working with the state's peak employer and union interests, those good practices and guidance. We have had a couple of people mention running small businesses. Those are the sorts of voices and practicality that we like to channel through, and those workplace concerns you have heard from unions and others can be channelled through as well. Guidance, information, support, and then evaluate the situation as it exists in the middle of next

year when we have further clarity on the wider regulatory environment. Please do not misunderstand us as saying you should pursue consistency with New South Wales. But we do understand it is one of the things you are considering.

Yoness BLACKMORE: On that—might I add, Scott—I remember now the review that was conducted by the select committee on the impact of technological and other changes in the future of work in New South Wales. Even in that review there they were saying that the New South Wales Act in itself was 20 years old and may very well need to be reviewed. It could be the case that a number of jurisdictions are having another look at their surveillance legislation in that sequential way at some stage next year.

John MULLAHY: Thank you.

The CHAIR: I am just mindful of time. I am sorry we will not have any time for further questions. Anthony is waving to me. Sorry, Anthony, do you have a burning question?

Anthony CIANFLONE: I am just curious to know—we have heard some amazing evidence from quite a few witnesses—what is Ai Group's view around the opportunity for artificial intelligence, AI, and even neurotechnology to potentially be rolled out into the workforce in the coming years?

The CHAIR: Sorry, Scott, just before you answer, I have got people waiting as well. The next people are coming through.

Anthony CIANFLONE: Sorry.

The CHAIR: No, I am going to let Scott answer, but I will just be timing him.

Scott BARKLAMB: I will be super quick. We did not hear the person on the neurotechnology, so we will take that on notice. We will have a bit of a think about whether we want to reply and will let you know.

As to artificial intelligence, I think perhaps the main thing we would want to stress is that we do not understand that that changes workplace surveillance. It is about a capacity to deal with and assess large amounts of information. I mean, correct me if you have heard something different, but for the most part you are still either listening or watching or looking at IT or vehicle tracking or location tracking, so the essence of surveillance does not change. Tools that allow employers to assess risks to meet their duties hopefully is where AI takes us. We would make no apologies for using AI to better understand risks, liabilities and duties to our employees and our commercial and fiduciary duties running businesses. It is a tool, like anything.

I will perhaps just finish with this point, Chair. The long history of workplace change and new technologies has had rightful concern about the impacts of changes, but in each instance those existing laws about that major change, which have been there from the early 80s, have proved robust enough to facilitate changes which have almost overwhelmingly led to more positive workplace experiences, to better workplaces and to better work, and we would hope that AI does the same.

The CHAIR: Thank you for that. Thank you, Scott. Thank you for your time today in answering some of our questions. We do really appreciate it. If there is something further that you would like to add, the Committee is more than welcome to accept any further information.

Scott BARKLAMB: Thank you. Can I just say a thankyou to your Secretariat. They have been absolutely fantastic in facilitating our appearance throughout.

The CHAIR: Yes, they are amazing. Thank you for acknowledging it, Scott.

Witnesses withdrew.