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

Chris Lehmann, General Manager, Membership, Advocacy and Partners, and

Georgia Holmes, Policy and Communications Advisor, Master Electricians 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 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 will remind members and witnesses to mute their microphones when not speaking just to minimise that interference.

Thank you so much, Georgia and Chris, for joining us today, for your submission and for taking some questions from us just to dive a little bit further into your industry and your thoughts around this inquiry. What I thought I might do is allow about 3 minutes for you to give a little bit of an opening statement, and then we will jump into questions. I will hand over to you. Thank you.

Georgia HOLMES: Wonderful, thank you. Good afternoon, Chair and members of the Committee. Thank you for the opportunity to provide our feedback on this important inquiry on workplace surveillance. Master Electricians Australia is the leading national trade association representing small and medium electrical contractors across Australia, and we are keen to emphasise the benefits of workplace surveillance for asset protection and ensuring a safe work environment.

Workplace surveillance tools serve a critical function protecting business assets and safeguarding the health and safety of employees. Maintaining the effectiveness of the current workplace privacy and surveillance laws is crucial for enabling organisations to meet their obligations of safety and asset protection. We want to emphasise that our members utilise workplace surveillance as investigatory assets and deterrence mechanisms towards third parties, not as instruments of control or constant surveillance of workers. Their primary purpose is to ensure safety and business efficiency, such as asset damage or unsafe work practices, while also deterring intruders and providing a confirmatory data source in the event of allegations of misconduct.

Importantly, our members do not intend to seek out minor infractions for punitive action against employees. Our members, who invest heavily in assets like vehicles, machinery and equipment, rely on these tools to ensure proper use of these resources as opposed to tracking employees' every move. Instead, they are used to verify incidents of damage or road violation, as examples, like speeding in company vehicles. Key to responsible use of workplace surveillance are transparency and communication. In our experience MEA members take this responsibility seriously. These tools are not designed to be deployed in a stealthy manner; instead, they are clearly communicated as part of an overall strategy to protect both the business and the workforce.

Surveillance also serves as a valuable tool in workplace conflict resolution, providing objective evidence that can help resolve disputes and address hostile work environments, offering a level of protection that can only be achieved through verifiable information. MEA urges protection for employers against the unlawful sharing of surveillance data with third parties. We highlight the risk of third parties gaining unrestricted access to footage which could compromise privacy and worker safety. MEA advocates for a balanced approach to ensuring employers' right to protect assets while limiting third-party access to viewing only, as opposed to copying rights.

In closing, MEA emphasises the need for a balanced approach allowing for employers to use surveillance for protecting workers in business while safeguarding privacy. We support clear regulations that ensure fair access to data and prevent misuse. We urge the Victorian Government to maintain a regulatory framework that respects employee privacy, allows responsible use of surveillance and does not overburden employers, ensuring a fair and transparent system for all parties. Thank you once again for this opportunity, and we welcome any questions on our position.

The CHAIR: Perfect. Thank you so much, Georgia, for that. I will jump straight into questions, because we have not got a lot of time. Dylan, I am going to go to you first.

Dylan WIGHT: Thanks, Chair, and thanks, Georgia. You touched on a fair few things there in a short amount of time, which was great. You spoke obviously about the fact that it is not your members' intention and it is not a practice of your members to use surveillance and data to unnecessarily monitor employees' every move. You also spoke about how it can be used to resolve some workplace conflict in some instances. We have heard some evidence throughout this inquiry about using workplace surveillance and the data collected, the issues that can arise or the issues that can exist when that is used for disciplinary purposes, I guess. And we have heard that one of the ways to sort of try and step through that would be giving employees access to the data that is collected on them and the surveillance that is collected about them as well—the surveillance that is being used on them as well—particularly leading into disciplinary procedures. Is that something that Master Electricians Australia would support?

Georgia HOLMES: Well, we are always very big on consultation with the employee and making sure they are involved in the process. I guess it would depend on the term of investigation that is being carried out, but yes, obviously that consultation and openness for the employee is a big part of our position on workplace policy, and it is part of our policy templates that we also provide openness and communication.

Dylan WIGHT: So what would that look like? We have heard instances where surveillance has been collected on an employee, they are brought into a meeting which ends up being a disciplinary meeting and they have had no access to that surveillance or that data prior to them getting into that meeting, which obviously puts them at a clear disadvantage in any sort of disciplinary procedure. Would you support them having access to that data and that surveillance before that initial meeting?

Chris LEHMANN: Could I just chime in there? I am the General Manager of Advocacy, Memberships and Partnerships here at MEA. Obviously if there was an issue and there was going to be a meeting, generally it would be around some sort of incident. Of course we would share that, but we would advocate for sharing that with an employee ahead of coming into any meeting. Really all we are looking at doing is protecting our member assets. I mean, I ran an electrical contracting business for many years and I did have geolocation on the vehicles. If people are doing things that they should not be doing with those vehicles, like after hours or going out of jurisdictions or taking them on holiday or whatever—they are company assets. We think it is completely appropriate that company assets, vehicles especially, should only be used for the purposes that they are allowed.

For workers who are working on their own, we are not suggesting that people have video cameras in vehicles and their every movement is videoed. It is really more location, so if someone is onsite and is there for longer than necessary or there is an issue, we can locate them. That is really for that health and safety process. And if as happened with me a couple of times when I ran my business, someone is taking the vehicle away on a weekend on holidays outside of the jurisdiction where they are allowed to take them and you end up with damage to a vehicle, then you would go back and look at if it had been somewhere it should not have been on the weekend. But we are not in any way, shape or form suggesting that there be extended monitoring. We would not be giving that unless there was an issue, and if there was an issue, we would be suggesting that you provide that to the employee ahead of any meeting. Does that answer your question?

Dylan WIGHT: Sort of, yes. I think it sort of gets to the point, but I had better let someone else ask a question. We have only got about 5 minutes left, I think.

Chris LEHMANN: Sure.

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

Wayne FARNHAM: Thank you. And thank you, Georgia and Chris, for your submission and for coming here today. A question I have got—it is becoming apparent through this committee that the data is owned by the employers most of the time. There was an instance where we had a person say to us around a WorkCover claim, where the employer had the video or the data attached to the WorkCover claim and the employee could not get access to that. What is your organisation's stand on this? Would you share a video with a WorkCover claim with an employee?

Chris LEHMANN: I believe I have answered that previously. Yes, if there was a disciplinary issue and we were using that footage or that geolocation data, we believe it would be only prudent and fair to share that with the employee, unless of course there was some legal advice by the insurer where we were not able to. But my expectation would be if there is an issue, it would be in most instances natural justice that people should be able to see whatever data is being used in a disciplinary process.

Wayne FARNHAM: I am probably not talking about discipline as such but more so how with workplace accidents quite often employees have to fill out that paperwork. The employer has the advantage of having the video. So what I am asking you then, and I will narrow this down, is if it is a workplace accident, would this organisation's employees have access to those videos?

Chris LEHMANN: Through whatever process—if it is WorkCover and if WorkCover insurance said that was okay or said that was prudent, we of course would. Quite often insurers have restrictions around these things. Our organisation itself would not have any issue in sharing that with an employee, but it would depend on what the rules were with the insurer and whether that was appropriate or valid to do so.

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

John MULLAHY: Thanks, Chair. Your submission refers to the Victorian information privacy principles, which only apply to public sector departments and agencies. Should similar requirements and principles apply to the private sector too, and what types of worker information should be protected?

Georgia HOLMES: As in terms of general data protection?

John MULLAHY: If we were to apply IPP to the private sector—so if what we have got in the public sector were applied to the private sector—what types of worker information should be protected?

Georgia HOLMES: Worker information—well, obviously all the privacy. From a high-level view, sorry, because our work relations team has more of the expertise on this, we would expect the privacy of an employee to be protected and applied over there. We are just looking purely to give a high-level investigatory tool if it becomes available. Of course we want all the workers' privacy rights to be protected. Is that answering your question? Hopefully.

John MULLAHY: I guess so.

Chris LEHMANN: Our focus in this is more around that asset protection and worker safety. Most of our members are smaller businesses. They do not have the sort of sophisticated systems that probably larger employers would.

John MULLAHY: Yes, okay. Thanks for that.

The CHAIR: Thanks, John. Anthony, I think we have got time for another question from you.

Anthony CIANFLONE: Thank you. I appreciate you guys appearing and your submission. We have not had that many employer groups or employers appear, so we do appreciate your time and definitely acknowledge that. I have gone through your submission again, which I appreciate, but just walk us through an example if you can from one of your organisations who are members in terms of how a worker is consulted or made aware of the technology around how they are monitored or tracked. I get the asset protection and the workplace safety side of things, but how is a worker made aware of that technology that is surveilling them? Do they have the opportunity to provide consent to having that technology on their vehicle or on their tools? How is their data stored by that respective member organisation generally? Then I guess picking up on some of the other questions, how can that data be retrieved at the request of the worker if they require it, and then how is it disposed of once that worker is no longer working for that member organisation? Could you just step us through that process at a high level?

Chris LEHMANN: We probably could not speak for all of our members, but the intention is when they are saying it is their vehicle it is not their vehicle if it is a work vehicle. It is an asset of the business, of the employer, and protecting that asset or the ability to be able to conduct an investigation into any damage both for their own insurance purposes but also if there is any sort of—God forbid—injury or accident with a vehicle is very pertinent and very useful. Because there is a heightened or an increased duty for employers to keep their

workers safe, quite often in the service industry you might have a single person in a vehicle, so it is knowing where they are and how long they have been there or if there is an issue. As I said, if you have got a job booked for an hour and 3 hours later they are still there and you have not had any call from them, knowing where they are would be very prudent and useful from a worker safety point of view.

In terms of how individual businesses would dispose of that, I cannot give you any clarity around that, but I would imagine in terms of consent it would be a workplace policy document. If you are driving a company vehicle or using a company asset, the ability to be able to monitor where they are as a tracking tool to make sure if there is an issue that help can be directed there would be in a policy document that they would sign—just like we get employees to sign for use of social media, use of employer assets, dress codes and all of those things. I know definitely that in the template documents that we put out at Master Electricians there is a template for things like workplace surveillance—'surveillance' is the wrong word I am searching for—or tracking of company assets and vehicles. Does that answer your question? Georgia might have a little bit more information on that.

Georgia HOLMES: Yes, just to summarise it, we do have a workplace policy that is available, so they have to sign a consent to that. I believe a lot of our members follow our policy templates. Whether they do that or not is obviously up to them.

Anthony CIANFLONE: So it is fair to say then that basically as far as you are aware employees are not proactively consulted about the type of technology and surveillance that they are then being asked to in a way automatically consent to as part of a broader suite of documents and measures in signing up to work for a prospective employer. They are not proactively consulted at the outset?

Chris LEHMANN: We represent mostly small to medium businesses. We are not your BHPs and your Rios or your tier 1 builders. They are not really the bulk of our membership. We think it is completely appropriate if it is a company asset and we have a positive obligation for workers' safety that that is a condition of employment when you are signing somebody up to make sure that employers can live up to those responsibilities and also that assets are protected.

The CHAIR: Sorry, Anthony. I am going to have to finish there only because of the time.

Anthony CIANFLONE: That is okay. Thank you.

The CHAIR: We probably could have asked a lot more questions. Thank you, Georgia and Chris, for answering some of our questions today—we really do appreciate it—and for the submission you made. Thank you.

Chris LEHMANN: We are very happy for any follow-up questions.

The CHAIR: Yes, that would be great. Thank you, Chris—and vice versa. If you would like to provide anything further if something has been sparked by today's conversation, we are happy to receive further information as well. Thank you for your time.

Witnesses withdrew.