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

James Fleming, Executive Director, and

Sunil Kemppi, Vice President, Employee Representative, Australian Institute of Employment Rights.

The CHAIR: I would like to start by acknowledging the traditional owners of the various lands on which we are all gathered today. I acknowledge that in this virtual environment we are all gathered on many parts of different lands, and I pay my respects to elders past, present and emerging.

I advise that the session today is being broadcast live on the Parliament's website. Rebroadcasting of the hearing is only permitted in accordance with LA standing order 234.

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

Thank you so much, James, for joining us this morning and taking a few questions from our committee. I thought it might be good if you could maybe start with an opening statement or a little bit of background particular to this inquiry, and then we will go to some committee members to ask you some questions.

James FLEMING: Sure. Thank you. Thank you for the chance to present to the Committee. I am the Executive Director of the Australian Institute of Employment Rights, which is a non-profit, nonpartisan think tank set up to promote fair and international labour standards. It is modelled on the structure of the International Labour Organization, so our executive committee is mostly volunteers and is made up of business leaders, trade unionists and independent academic experts. I will hopefully be joined by my colleague Sunil Kemppi. He is having some PC issues logging into Zoom. He is one of the vice-presidents and Employee Representative.

The CHAIR: Great. Thank you so much, James. As a committee, we understand you have done research. We have been doing this committee hearing with submissions coming to us and with other hearings delivering evidence. We might ask you a few questions just to start us off, in a bit of a background sense, on some of the work that you have been doing and then we might get into some nitty-gritty as well. I might go round and just introduce the Committee to you quickly as well.

We have got Wayne Farnham, who is the Member for Narracan; Anthony Cianflone, Member for Pascoe Vale; Dylan Wight, Member for Tarneit; and John Mullahy, Member for Glen Waverley.

I will go around those on my screen. Wayne, I might go to you first if that is okay.

Wayne FARNHAM: Thank you, Chair. Hello, James. Thank you for attending today. This one has been an interesting space. I think it is the first time you have probably had a committee talking about workplace surveillance and AI and various things. I will get straight to it: how have you seen recent trends in workplace surveillance? Have they improved or diminished, and what about productivity and safety?

James FLEMING: Thanks for the question. We have been monitoring, researching and writing about the broader digitalisation of work, and this year we are hosting a debate on AI in work. But back in 2021 we hosted a podcast on algorithmic management, and so it has been on our radar since then. One of the worries is that on the one hand, with the great digitalisation of work—you know, the production of more and more digital tools for managing work—there is a greater capacity for surveillance and for algorithmic management but at the same time there is very little empirical data, as you have probably found as a committee, on how prevalent this is and how exactly it is being used. A lot of it is anecdotal. I was going to suggest, if the Committee has the capacity, that it would be really great to commission some empirical work on that. One of the limitations of course would be that often employees might not know that they are being surveilled or how that is happening. But a lot could hopefully still be gathered through that kind of process. We could go conceptually into what our concerns are about it, but how would you like me to proceed?

Wayne FARNHAM: I have got to give other MPs the opportunity to talk as well. Otherwise you could probably spend the whole time answering my question. But I suppose just as a quick follow-up on that, where do you think the balance is?

James FLEMING: Sure. Maybe I will just say one thing to answer your previous question specifically. A lot of the concerns that we have heard about have been coming through from rideshare drivers who are surveilled and gig workers who are getting work through apps and often being managed through algorithms. Our concerns are about how being managed in that way means workers can be alienated in the workforce and not know the kind of mechanisms that are going on in the background.

At the Ron McCallum debate last year we had an Uber driver talk about his experience of being cut off from work altogether because of an unfair user review. So workers are being performance managed, effectively, through user reviews and then how algorithms use that. The algorithms are used, we hear, within this industry to rank drivers and allocate them more or less preferential work and put them higher up the waiting list, but the worker does not have access to this data or have any influence and cannot consent to how it is used and does not have protections around that.

In terms of where the balance is, I should say from the outset that I think these tools are not inherently bad and that data-driven management decisions could be a good thing, but it is all about protections around that data and making sure it occurs within a well-regulated environment to minimise the risks and harness the opportunities. We have some suggestions about how that regulatory space could look and what kinds of protections there need to be. But there is enormous potential to exacerbate the inherent power disparity between the worker and the employer or the supplier of work. In order to ensure that there is a balance there needs to be better worker involvement in how these tools are implemented—for example, through consultation and through consent. Also because consent is not enough, given the power disparity, there need to be some objective limitations on how these tools can be used—some kind of proportionality or reasonableness protections like what we are hearing talked about in the privacy law space. In the Uber driver example, for instance, the worker is often, because of the power disparity, only able to accept the job on whatever conditions the employer dictates, so the consent is sort of meaningless. The only real choice they have is to take the work or leave it. So there need to be some objective reasonableness requirements about this data and the kinds of purposes it can be used for.

Wayne FARNHAM: Thanks, James. I will let one of my colleagues have a question.

The CHAIR: Thanks, Wayne. I will go to you, Anthony.

Anthony CIANFLONE: Thank you for appearing, James. My question is around artificial intelligence. Several submissions have mentioned the use of AI and algorithmic decision-making based on surveillance data and performance management. So what are, in your view, the risks? You touched on a session you have got coming up I think on AI specifically, which sounds interesting. But how do you think these AI risks can be mitigated and foreshadowed in any recommendations we may be able to make as a committee on this issue?

James FLEMING: Thanks for the question. So yes, it could be the top-down power structures within the workplace that have the potential to really alter the employer–worker relationship and kind of circumnavigate some of the IR protections that we have. We do not see it as inherently bad. It all depends on how these tools are used and whether it is done in a balanced way, as I was saying, with worker input and consent. But some of the things that concern me in the rideshare situation are around where things are completely automated. There still needs to be recourse for review and oversight, and in that context there often is not; the work is entirely dispatched through algorithms, decisions are made and a person can be cut off from work. That does not seem to be a problem with AI itself; it is in how it is being utilised.

So how do we ensure that we minimise the risks and harness the opportunities? I mentioned that we should look at those debates around the Privacy Act changes. Perhaps my colleague Sunil, who is now joining us, can talk a bit more about that. But there needs to be some kind of objective reasonableness requirement and the opportunity for consent—but consent is not enough. Also the Committee could look—it probably already has—at the greater privacy protections and protections around the use of personal data that apply under the GDPR in Europe. It seems at the moment in Victoria the Privacy Act does provide some relevant protections for the use of personal data, but they are not as extensive. For example, from what I understand there is no requirement for explicit consent to the gathering of this data or for the use of AI algorithms and this kind of

algorithmic management. There is no right to have a copy of the data, to get it in a portable form or to have it erased, and the GDPR system has much more extensive penalties.

There should also be some objective requirements around the purposes of the surveillance. I notice, for example, there is some scholarship around the use of worker surveillance back in the gold rush era, and I can forward the Committee the reference, but apparently at that time in the late 1800s in Western Australia there was worker surveillance going on to try and prevent the theft of gold, but then that was later used to quash collective organising and trade unionism. So you do want to make sure that it is being used for legitimate purposes.

The CHAIR: Thanks, Anthony, for that question. And I welcome Sunil as well, who is joining us today. Sunil, I am happy for you to jump in if you want to add to any of the questions. Dylan, I might go to you next.

Dylan WIGHT: Thanks, Chair. And thanks, James and Sunil. So what we know is that New South Wales and the ACT obviously have specific workplace surveillance laws. Do you think Victoria should be following their lead—and not just following their lead in terms of creating their own workplace surveillance legislation, but do you think those two models are sufficient or are there ways that they could be improved if Victoria was to go down the route of legislation?

James FLEMING: Thank you. I am not familiar with those models in those states, being from Victoria myself, but perhaps Sunil has something to say on that point.

Sunil KEMPPI: Thanks. Yes, I will jump in on that one. I will be very honest and say it has been a little bit of time since I have truly acquainted myself with those laws. But I do remember once I had to do an exercise where I had to work out, for an employer of mine at the time, what would be the case in terms of the telephone software where you can track the location of the phone, and it was about asset protection, not necessarily seeing where people are. I remember we were a national organisation and I had to give an answer that was 'If the person is in Victoria, it is X answer; if the person then cross the river to New South Wales, then you have to put a label on the phone; and in South Australia it would be a different thing again' et cetera. One of the things I would say on that then is, yes, I think Victoria needs to have some laws about worker surveillance and data, generally speaking. I think it is a much broader issue than surveillance per se as you customarily understand it in the sense of, say, video cameras and that kind of thing and probably more of a law about data gathering, the use of data and the disclosure of how that data is gathered and used et cetera. But going to my earlier point, admittedly by way of anecdote, I think it is important that if Victoria is to have a law about this, it ought to be one that is consistent with the body of law that exists in the Commonwealth already, or in other states and so on, to the extent possible.

Dylan WIGHT: So in terms of that, when you are talking about surveillance and data and whatever, that is essentially just how you are going to define surveillance in your legislation, I would think. I take your point about having not uniform but I guess similar laws for the purpose of making it easier and streamlined for the businesses that operate nationally. To that point, do you think the best model would be for Victoria to have standalone legislation in terms of this sort of stuff?

Sunil KEMPPI: Yes, I do. I think that there is a need for some sort of regulation in this space. It is a very under-regulated space. I also think that surveillance, as we customarily understand the phrase, probably is not the right term. We are really talking here I think about the use of data, the collection of data and the broad swathe of things that go beyond simply surveilling somebody in the common sense of the word.

The CHAIR: Thank you for that. John.

John MULLAHY: Thanks, Chair. And thanks, James and Sunil, for turning up today to our hearing. We heard evidence earlier from a few unions with regard to surveillance being used to get rid of workers, essentially, and the worker having available to them only a small proportion of the actual surveillance that the employer wanted to use. What safeguards should Victoria set up to keep employers accountable for their surveillance activities?

James FLEMING: Perhaps I could start on that. Turning to the GDPR in Europe, it would be advisable I think that employees have a similar right to a full copy of the data, and in a form that they can use. They should have a right for it to be erased, and the data in the first place should be limited by some sort of reasonableness

requirement about what can be collected and what cannot. And that should be challengeable if there is some kind of ombudsman, government regulator, supervisory body, privacy commission or something of that nature.

Sunil KEMPPI: Just to add to that slightly, again going to that earlier point that I was developing. Surveillance as it is commonly understood might be that the employer has video cameras in place and they have staff working in that place and they use those video cameras to point to some aspect of conduct. But surveillance these days is so much more broad, and it is being exacerbated by emerging forms of technology. We know from, say, the US that surveillance, perhaps not as it is commonly understood, is being employed to [Zoom dropout] or look at the communications that are sent between workers unbeknownst to those workers. If you were to do a survey now asking employees 'Have you been surveilled by your employer?' or 'Do you know that you're being surveilled?', most of them will say no despite the fact that perhaps they are. Surveillance can also take the form of noting where a particular person is at a point in time, and it can then be used to say that person is moving too slowly—through a warehouse in the case of Amazon.

I think that one of the ways to get around this would be to ensure that employers have to tell people that they are being surveilled, the way in which they are being survived and how that information will be used—so there is a disclosure requirement there. To go to the point that James made earlier, it has to be more than a simple notification at the point at which a contract is formed, which is the complete manifest of the power dynamic—or the imbalanced power dynamic. One of the ways to do that would be to regulate it through, say, collective agreements or some sort of collective form of negotiation between the employees and their representatives with the employer as to how data will be collected and used—whether it will be—et cetera.

Then of course there is the [Zoom dropout], which probably is a matter for perhaps even the Evidence Act—how data can be used, how it can be gathered and whether there are any restrictions on, say, for example, improperly obtained data being admissible in court proceedings and things like that. So it is really the start of the spectrum, how it is gathered and how it is used, and then it goes all the way to the ultimate use of that sort of information.

John MULLAHY: I know we did have evidence on how you can get app updates for different tracking software and things like that which have different types of new surveillance that can be used and so you have to have that ongoing conversation with your employees.

Sunil KEMPPI: Yes.

James FLEMING: If I could just respond quickly to that, the regulation should be proactive and not reactive. As we just heard, there are difficulties. Technology and business practices are changing so rapidly that we need regulation that is going to work no matter what the details are or how those developments play out.

We have some ideas about that and a sort of philosophy of regulation that might be relevant to the Committee in our recent book, *A New Work Relations Architecture*, which draws on the principles behind the work health and safety system. Instead of having very prescriptive regulation, you can point to broader objectives and put the responsibility on the parties in the workplace to come up with a way that makes that fair. If you have a general requirement and an objective that the gathering of this data has to be, for example, reasonable, proportionate, fair and clear purposed, then it puts the responsibility on the parties to work out what form that would take, because as was hinted there, if you are too prescriptive, it is going to be quickly out of date.

The CHAIR: Thanks for that, James. I might do a quick follow-up question to that about the biometrics and the advances that we are seeing in surveillance, including tracking, facial recognition, fingerprinting or even workplaces asking for blood samples or the health records of their workers. I wonder whether you have got anything around the protection of that biometric data as something that we should be doing here in Victoria.

James FLEMING: I think similar principles apply. It has to be reasonable, for a clear purpose and the employee has to explicitly consent, but consent is not enough, and they need to be able to get access to it. Around health and such highly personal things, I wonder if there should be some absolute restrictions, but I have not turned my mind to what form they would take. There could be some detail there about what things are reasonable in relation to health and one's body. Without trying to predict the technology, it is hard to imagine how gathering someone's DNA, for example, could be at all relevant. Also, if it is data that could inherently be used for a discriminatory purpose—the way we have it under the Privacy Act in Victoria is that there is a

prohibition on even gathering information that might be used for a discriminatory purpose. There might be some categories of data you would want to exclude altogether.

The CHAIR: Yes. That makes complete sense. In that sense, about what is reasonable and proportionate, are you seeing or having evidence that excess surveillance actually has an impact on workers' mental health or their physical health?

James FLEMING: Perhaps, Sunil, if you want to respond to that point.

Sunil KEMPPI: Thanks. What I will say on that is that one of the issues, ironically, in terms of the mental health impact is that many workers would right now not know if they are being surveilled, so it may not have a mental health impact until the point at which it bites, which is when they are confronted with, 'You sent this email to this person' or whatever the case might be or, 'Here you are on camera' et cetera. So there is probably a large group of workers whose mental health is not being impacted despite the fact that they are being surveilled. However, there is also a large group of workers, for example, in obvious places, like places that are surveilled using video technology, that constantly feel like they are being watched. Then there are less obvious examples where office workers have had annual leave deducted because they sat at a different desk, for example, at the bank that they work for. That has an obvious mental health impact. Knowing that an employer knows where you are at every second of the day has an obvious mental health impact on people.

Then there are, beyond mental health, quite physical health and safety elements to this as well when you think about the algorithmic management and the data points that are collected about where workers are at a particular point in time. At, say, rideshare and delivery companies there are, to be frank, actual worker fatalities commonly reported simply because people are rushing the order or rushing the job or rushing to get to the next job because the algorithm pinpoints where they are at every step of the way. So, yes, the health and safety impacts flow from very physical, real impacts to less seen but longer term impacts also.

James FLEMING: If I could add just briefly, if it helps the Committee, I think the rideshare driver Syed Mubashir, who spoke at last year's Ron McCallum debate and who has become an activist for other rideshare drivers, spoke very eloquently about the personal impact on him of his algorithmic management and the way it he was being surveilled. I could send an extract from the transcript of that if you want some evidence of that kind of impact.

The CHAIR: Yes. That would be really helpful. Thank you. That would be excellent. I am just mindful of time. I think we just have time for one more question if we can. I will go to you, Wayne, again.

Wayne FARNHAM: Thank you, Chair. I will come back to the balance I was talking about earlier. If I had to play devil's advocate here, I would say the employers will say one thing and the employees will say another thing, and I can understand both sides of the argument. But what I am really getting to is: what impact does the unreasonable workplace surveillance have on workplace relations and the balance of power between the employer and the employee? I can see this imbalance occurring. What are your thoughts on that?

James FLEMING: Thanks for the question; it is a good question. One of the impacts is that it can facilitate a whole new form of work where the worker is completely alienated from the workplace—where there is no workplace and they are completely alienated from each other. If you are just working through an app doing gig work and your work is being managed by a machine, then you do not have access to collective representation, to unions or to your colleagues to try and push back against that inherent power imbalance. So it is a whole new form of work that is even more imbalanced because of this alienation, I think. But also it can feed into the top-down power structure. Surveillance is one way, so it is more power the employer has. Potentially, if it is not used properly, this data is tipping the scales further by gathering information, giving the capacity to micromanage workers and employees. It could be used to discriminate against them behind the scenes. Was there anything that you wanted to jump in with on that, Sunil?

Sunil KEMPPI: I might just jump in and say that surveillance in its essence is an inherently collective issue. It is an issue that affects groups of workers as groups of workers. A lot of the solutions and a lot of the regulatory framework are directed at the rights of particular individuals, and the law falls down when it comes to those rights that individuals have to not be surveilled, partly because of the inherent power dynamic in the employment relationship. So when people sign employment contracts, for example, they sign away their privacy rights because of course they want to work and to have a job, and for that reason, drilling down perhaps

beyond your question, the solutions here probably need to be ones that take into account the collectivism, generally speaking, and look towards how it is that groups of workers can negotiate with employers and regulate their data, how it will be used and how it will be used for them or against them et cetera—how it will be stored, how it will be used and so forth. So yes, we are of the view that it is a collective issue that needs a collective solution.

Wayne FARNHAM: Thank you.

The CHAIR: Thank you so much to both of you for your time today. We really appreciate you answering our questions and helping this committee with deliberating on this. Really it has been an interesting topic, and you have added today to that discussion, so thank you so much. James, yes, if you would like to send anything further to us for the Committee to consider, we will welcome that as well. Again, thank you so much for your time today.

James FLEMING: Thank you, Chair.

Witnesses withdrew.