T R A N S C R I P T

LEGISLATIVE ASSEMBLY ECONOMY AND INFRASTRUCTURE COMMITTEE

Inquiry into workplace surveillance

East Melbourne – Monday 23 September 2024

(via videoconference)

MEMBERS

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

WITNESSES

Associate Professor Penelope Williams, Director, and

Danae Fleetwood, Master of Philosophy research student, Centre for Decent Work and Industry, Queensland University of Technology.

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 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 that interference.

Thank you so much, Professor and Danae, for coming along today to speak to our inquiry. I am happy to give you a few minutes if you would like to speak further about your industry or give us a bit of insight on what work you do, and then we will jump straight into some questions.

Penelope WILLIAMS: Thanks, Alison. I might start if that is okay. Firstly, I would just like to thank you for the opportunity to participate in today's hearing and for your interest in the submission made by the Centre for Decent Work and Industry. As you can see on the screen, I am Associate Professor Penny Williams—and you can call me Penny today—and I am the Director of the Centre for Decent Work and Industry, which is a research centre based in the faculty of business and law at QUT. The Centre for Decent Work and Industry is an interdisciplinary group whose research encompasses responsible governance in industry, transitions in and out of work, how work is changing—particularly new contexts for work, such as the gig economy—and how technology is shaping work. We particularly consider how these issues impact worker rights, wellbeing and the gendered and intersectional dimensions of workers' experiences.

My personal interest in technological change at work has come from both my academic research and my prior experience in industry as an HR professional. Last year I was awarded an Australian Research Council grant to investigate the automation of people management and the use of AI and algorithmic management in traditional workplaces. This research, which is still in progress at the moment, informs much of our submission to this inquiry. In particular this research points to a flourishing market of off-the-shelf and tailored human resource management technologies that incorporate various forms of workplace surveillance. These are multifunctional HR systems that can operate through a variety of digital devices, and they draw on significant amounts of worker-generated data that is gained generally through various forms of overt and sometimes covert surveillance of workers. While these technologies are not purely adopted for surveillance reasons—that is often not the main reason for their adoption—their surveillance capabilities are significant, and they are not currently regulated by surveillance laws in Victoria and much of Australia.

The research grant that I have also supports research by our master of philosophy student Danae Fleetwood, who joins me here today. I am going to let Danae just briefly introduce herself and her research before handing back to you for questions to us.

Danae FLEETWOOD: Thank you, Penny. As Penny mentioned, my name is Danae Fleetwood, and very relevant to today, I am studying the regulation of workplace surveillance in Australia, with a particular emphasis on AI-enabled monitoring technologies. Prior to my study I have a background in HR and ER and as an ER adviser for an employer association, so my interests draw on the balancing act between the needs of employers and the protections necessary for employees. When I first started my study and working with Penny it quickly became evident to me just how lacking the regulations are around the use of AI-enabled workplace surveillance in Australia. I initially thought there must have been something I was missing, but considering the role of work health and safety laws, discrimination laws, employment laws and privacy laws, there is still a significant gap in this area that needs to be filled by workplace surveillance laws. So whilst, as you are aware, all states have some form of surveillance laws in place, such as the surveillance Act in Victoria, not only are these statutes entirely inconsistent, with varied terms applicability, but they are also not developed and equipped to regulate the types of surveillance that we are seeing being continually developed today.

Likewise, since the hearing has been going on we have had the amendments to the Privacy Act announced, and they have failed to extend the operation of the Privacy Act to employee records. As such, we see this as a really positive and necessary step towards the ongoing protection of workers rights and an opportunity for Victoria to lead the way in establishing a responsible approach to these concerns we have around workplace surveillance. Thank you again for the opportunity to address the Committee, and we welcome any questions you might have.

The CHAIR: Perfect. Thank you so much, Penny and Danae. I feel like we are doing work in a very concurrent space at the moment and your insights are going to be very vulnerable to our committee, so thank you for that. Kim, I might go to you first, for the first question.

Kim O'KEEFFE: Thank you. It is a very interesting submission. I really appreciate it, and you both have a lot to offer to us to get a much better understanding. Probably my question you have touched on a little bit. Your submission acknowledges the legitimate reasons employers use surveillance. At what point would you say surveillance becomes unreasonable?

Penelope WILLIAMS: Perhaps if I start, Danae, then maybe you can add to that. This is a difficult one, but I think where surveillance becomes unreasonable is when it is constant, when it occurs in an employee's personal and non-work time and when the surveillance involves gathering data that is not specifically related to the job requirements that the worker is doing or to the protection of the data security of employers in the process of doing that. The unfortunate thing is that a lot of the technology that is available now is available on your phone or on your laptop—and a lot of the wellbeing apps that are being developed now might also monitor your non-work health and wellbeing behaviours—and there is not really any guidance for employers on how to use that data, how to protect that data or when it is appropriate to use that data. That poses risks for employees as well as employers. It is those boundaries around the personal and professional life and around the relevance of the surveillance to the work that the worker is doing.

Danae FLEETWOOD: Just to pick up on that point that Penny finished with, the relevance is a core function here as well. So the same surveillance technique may or may not be legitimate depending on how and why an employer is using it. For instance, if they are using it in stealth mode covertly without acknowledging it to the employee, it is going to be a lot less legitimate than if it is an announced, consulted policy in place with clarity around how it has a reasonable managerial purpose. So it is more about the way in which they are responsibly utilising it, as opposed one size fitting all in that.

Penelope WILLIAMS: Perhaps I will just add to that by saying, for us, the key to that is transparency.

The CHAIR: Yes, and that has been raised by others as well. Thanks, Penny. John, I might go to you next.

John MULLAHY: Thanks, Chair. Thanks, Penny and Danae, for turning up today with your evidence. We have had earlier evidence from union groups that look after people in the banking sector basically stating that many of their members were getting a limited amount of evidence of things that they have been doing wrong. There was no presentation of all the surveillance provided to the workers. Your submission states that employees have little recourse if they feel that workplace surveillance has infringed on their rights. What mechanism do you think would work best to enable employees to raise their concerns or seek redress?

Danae FLEETWOOD: I will perhaps start with that one. For me, this is a major area of my research. I am currently looking at what can actually be done to help employees with this. A lot of the case law I am looking at finds that even if there is surveillance and there are potentially some laws in place and it has been done unlawfully, matters have then gone to the Fair Work Commission, perhaps relating to an unfair dismissal claim, and the Fair Work Commission is not bound by the rules of evidence. Even if they were, they essentially find that that evidence has high enough probative effect that they admit it, so that creates a problem. People are going to use it anyway, because ultimately the reason that they are using it is not preventing them. In lieu of that, I think having in place systems like the workplace surveillance laws in the ACT, where there is a consultation process, having in place policies and having in place mechanisms by which employees can actually voice their concerns, either directly or through collective bargaining, around the concerns and the means by which they are being regulated, will help aid in the actual initial rollout and then prevent those issues further down the track.

The CHAIR: Perfect. John, do you have anything to follow up? No. Thank you for that question. Wayne, we will go to you.

Wayne FARNHAM: Thank you, Chair. Thank you, ladies, for presenting this and coming here today. Out of everyone on this committee, I am probably the biggest fossil when it comes to AI and algorithms. I am not right up to speed with it, but probably what I am curious about is how artificial intelligence and algorithmic decision-making is changing workplace surveillance and what regulations are needed to prevent any negative effects from that.

Penelope WILLIAMS: I will perhaps take the first half of that question about how it is changing workplace surveillance and then Danae might want to chime in with the regulatory components. I guess the first way that AI and algorithmic decision-making is changing surveillance is through enabling more subtle and pervasive forms of monitoring. So basically, AI and algorithmic decision-making, or automated decision-making, require data in order to drive the decisions or the recommendations that are made. To gather this data requires some form of monitoring of worker behaviour, which requires some form of surveillance. It is a necessary part of the technology in order to gather that data. If I can give you an example, there are a wide range of software and technologies that are designed for various forms of people management, and they might do things like time and attendance tracking or they might do rostering and scheduling or what is commonly now called workforce optimisation. They might measure the productivity of workers and produce reports on how quickly work is being done, but they might also automate things like the allocation of tasks or the tracking of task completion. Now, these things in themselves are not bad. In fact the automation of these things is really good for Australian employers and organisations, because if we do not automate those very manual processes, it affects our economic ability to be productive and competitive on a global level. I think in themselves those functions are not necessarily problematic.

What happens is that they also have to surveil workers in the process of doing this, and generally these technologies do not just do scheduling and rostering. They might also identify data security risks from employees, whether they are deliberate or inadvertent—you know, downloading information they should not be—and they often rank employees on a leaderboard based on the time they have taken to do something or their productive work. This can be problematic because it really just brings all of our work down to time: we are currently being measured on how quickly we get a task done. What we are hearing in our research and certainly also from union representatives that we have talked to and workers that we have talked to is that that can result in some workers feeling that the quality of the job is not being acknowledged and that they are being pushed to work harder and faster. As we have even seen in the gig economy and in the case of contractors in warehousing, it can even relate to whether their contract is renewed. This is where it becomes a double-edged sword. We need automated decision-making and AI in order to improve our existing systems, but if we do that without considering the sometimes unintended consequences of that, we might inadvertently erode the work conditions and the rights of employees in doing so. That is why regulation is needed. Perhaps, Danae, if you want to just briefly touch on the types of regulation we think are needed.

Danae FLEETWOOD: Yes, of course. As Penny was touching on then, these devices are not for these singular surveillance functions, like we see in the legislation at the moment. The general surveillance laws in Victoria, for example, cover optical listening and tracking devices. For tracking devices, it states that it specifically has to be the primary purpose for which that device exists. That is problematic when we have a device that has many functions, as we are seeing in these systems. These separate components also become problematic when we have a system which consists of perhaps a wearable with a computer function also connected to it. It starts to blur the lines, for example, of 'Is this an optical device? Is this covered by these areas?'

In some of the other states, in particular with the workplace-specific laws in the ACT and New South Wales, they have taken the next steps to cover data surveillance devices. They do a lot better in covering a lot of these more modern technologies. But we still think that having something like a technology-neutral terminology that allows for the current and future development in this rapidly changing area, where we do not fully understand what tomorrow will be, will help to futureproof that. Even in I think the New South Wales workplace-specific laws in relation to optical devices, the way in which it is worded kind of implies that it is only applicable to CCTV—there is a requirement to have signage et cetera. So it is not quite at that futureproof stage that we think is appropriate.

Wayne FARNHAM: Thank you for that. I appreciate it.

The CHAIR: It is an interesting space about those blurred lines, and that has been raised throughout the Inquiry as well. Anthony, I think we have got time for another question from you.

Anthony CIANFLONE: Thanks for appearing. Just building on that, I am interested in your views around what you describe in your submission as 'technology-neutral laws'. Many submissions, including your own, support workplace surveillance laws that apply to current and evolving future technologies and what is encroaching on those blurred lines. But can you give any best practice examples, whether across the country or internationally, namely, that you think we should be considering or looking towards in framing up potential recommendations in this space for Victoria?

Danae FLEETWOOD: This is certainly a question that our colleague Andrew Stewart could best answer. He has phenomenal understanding in this area. But my very brief version, and Penny might have something else to add, is: looking at the level of risk is a consideration seen overseas—so the high risk, you know, what sort of data and what sort of information is being collected and having that as a consideration. But technology-neutral is really about regulating the process. It is that there is surveillance and understanding what 'surveillance' means, and then any device capable of doing that can be covered. It prevents those definitive lines around what is in and what is out and gives the potential, maybe, for common law, or case law, to develop over time as needed. It allows the legislation to be something which can continue to evolve with a future that we do not fully understand. I am not sure if Penny has anything to add on that.

Penelope WILLIAMS: I do think there are potentially some examples that can be drawn from. For example, the ALRC, the Australian Law Reform Commission, does have some recommendations around surveillance being technology-neutral. They have some kind of guidance on what they consider to be technology-neutral. I think that provides a good starting point to think about. I do also think that some of the work that has been done within and some of the definitions that are applied in the New South Wales legislation or regulation around workplace surveillance may provide a starting point for Victoria to consider as well.

It is a difficult one, and it is a moving feast. I think the important thing to remember is that regulating for workplace surveillance does not necessarily mean regulating for everything that might happen or arise out of workplace surveillance. For example, the potential for discrimination that might occur through workplace surveillance might already be covered by provisions under the Fair Work Act. So there are other mechanisms that can be applied. The problem is that in a lot of cases at the moment employees do not know that they are being surveilled and therefore that decisions might have been made based on data that they did not know was collected.

The CHAIR: Yes. Penny, I just want to quickly ask a question around the technology. I feel like I cannot keep up with the technology that gets rolled out on my own phone. But your submission talks about, in New South Wales, the prohibiting of the manufacturing or supplying of a device that is intended to be used that actually then contravenes the Act. Can you just talk a little bit about that and how that works in New South Wales and what we could learn for Victoria?

Danae FLEETWOOD: I can talk about that. In New South Wales they have a provision—I do not have it on my screen at the moment, so I am just going to ad lib—in relation to the manufacture and supply of surveillance devices if the manufacturer or supplier knows that it is going to be used for an unlawful purpose.

The CHAIR: Right.

Danae FLEETWOOD: That is obviously a little bit grey in itself, just by its very nature—how can you know that it is going to be used for an improper purpose? But what I have seen in some of the technologies that I have been looking at—I have looked at their websites et cetera—is that particularly around international laws they are making an effort to show that they are complying with them and to show how they are fulfilling those requirements there. I think if this were more widespread in Australia, it would be similar—'Our technology complies with workplace surveillance laws because we ensure that X, Y and Z,' or it might encourage users not to use it for those improper purposes. In itself I am not sure how effective it is at saying, 'We knew, yes or no,' and actually finding a contravention. But it might have more of an encouragement effect for manufacturers to provide a little bit more warning and education to their users around the laws.

The CHAIR: We heard at a previous hearing that they would take a technology or something, and the employer would then work out, 'Oh, it did X, Y and Z as well. We didn't realise that, but now we could use that.' Are you seeing that as well?

Penelope WILLIAMS: Yes, we are. I think in general most organisations do not use all the functionality of any technology that they have; they only use a portion of it. What is interesting about the new human resource management or people management technologies is that they do have extensive capabilities. We are seeing that they are using it for a wide range of things. I think Danae gave the example earlier of where keystroke tracking was used to evidence the underperformance of an employee, but that technology was not necessarily purchased for that purpose. It may have been purchased just to manage data security risks within the organisation. This is where banning the manufacture can become problematic—or putting the onus back on the manufacturer as to what is a banned use or not. But that is not to say providing similar provisions would not strengthen the regulatory framework and also provide some guidelines for the users of the technology as well as the manufacturers.

If we look at what is being proposed and what has happened in the EU in relation to artificial intelligence, they have identified high-risk scenarios, such as the use of AI for recruitment and selection of employees, where the implications are so significant for the worker or the person that it should not be used in that context. So, yes, we are definitely seeing that, and that is why we do think that even though it may not always be easy to enforce, it is worth implementing something along these lines.

The CHAIR: Perfect. Thank you. That time has just flown. I feel like we could keep chatting all day. Sorry, we are going to have to wrap it up there. We really appreciate your research and the work that you are doing and you assisting the Committee today as well by answering our questions. Thank you so much.

Witnesses withdrew.