T R A N S C R I P T

LEGISLATIVE ASSEMBLY ECONOMY AND INFRASTRUCTURE COMMITTEE

Inquiry into Workplace Surveillance

Melbourne – Friday 1 November 2024

MEMBERS

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

WITNESSES

Sarah Roberts, Secretary, Victorian Division, and

Associate Professor Alysia Blackham, National Tertiary Education Union;

Lauren Kelly, Research and Policy Officer, United Workers Union; and

Alana Ginnivan, Professional Officer, Victorian Branch, and

Libby Muir, Professional Officer, Victorian Branch, Australian Nursing and Midwifery Federation.

The CHAIR: Welcome to the panel 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.

We are going to run this session straight into a question-and-answer-type format and committee members will ask some questions. If you wish to answer that question, just raise your hand, maybe state where you are from at the start, and then we will just have a conversation as we go. If there is anything that is not raised or if there are important points that you do not have an opportunity to speak to today, you are welcome to provide additional information or a submission to us in writing.

I will quickly introduce the Committee—they will introduce themselves—and then we will go straight into it, if that is okay with you. I am Alison, the Member for Bellarine.

Kim O'KEEFFE: Welcome, and thank you so much for your submissions. I am the Member for Shepparton Kim O'Keeffe.

Dylan WIGHT: How are you going? I am Dylan, the Member for Tarneit.

Anthony CIANFLONE: Anthony Cianflone, Member for Pascoe Vale.

Wayne FARNHAM: Wayne Farnham, Member for Narracan.

John MULLAHY: And John Mullahy, Member for Glen Waverley.

The CHAIR: Thank you very much. We are going to go straight to questions, because we have got a little window to chat with you. Kim, I am going to go to you first.

Kim O'KEEFFE: Thank you so much. My question is: in what ways are existing privacy and workplace surveillance laws failing to protect workers from excessive surveillance?

The CHAIR: It is a big one.

Alysia BLACKHAM: I might start. Alysia Blackham. I am an associate professor at Melbourne Law School at the University of Melbourne and a member of the NTEU. At the moment the way that data privacy law is structured leaves a gaping hole for employment and employment records. Federal law has a very large exception for small business, so anything with under $3 million in turnover is effectively exempt. They have committed to reviewing that, but they have not done so. In terms of the workplace, there is a gaping exception for employee records, so employee records, once they are collected, are not subject to federal privacy law. At the state level, while we have data protection law for the public sector, there is nothing in the private sector, so essentially with Victorian small business in the private sector, there is no data protection law that covers those entities or those workers, and this is a massive gap in regulation. So in terms of data privacy law, there is basically no coverage for these organisations and for these workers, so that is a real challenge. We do have some surveillance legislation in Victoria, but it is very narrowly targeted at certain types of technologies and certain contexts, like bathrooms. This is not enough to protect workers, particularly as digital technologies continue to evolve.

Kim O'KEEFFE: Thank you. Does anyone else want to add?

Alana GINNIVAN: Good afternoon. My name is Alana Ginnivan. I am a Professional Officer from the ANMF Vic branch. We service over 106,000 nurses and midwives within Victoria alone. We also agree and experience from our members' perspective the commonalities experienced of the lack of protections for data privacy. As we know, there are portions of the legislation that refer to areas of protection such as bathrooms, lactation, breastfeeding et cetera. The unique experience of our members is that images and data that are collected are commonly obtained in areas that are deemed personal and private information in a healthcare

setting. So what that means is it exposes not only the workers, being the nurses, midwives, carers; it also exposes the broader public to subjective laws that do not exist—or policy procedure, my apologies—so what we do experience is that workplace surveillance has expanded. We know that, but it is being utilised in ways that are punitive and/or beyond employees' control, and it does not expose just the workers; it is also the broader community.

Lauren KELLY: May I add a short comment. My name is Lauren Kelly, here representing the United Workers Union. We have about 130,000 members across 45 industries, and a lot of our workers are experiencing coercive surveillance technologies face to face within the workplace itself. Really what we find is beyond just issues of data collection; as well there is a real shift in management world view or attitude that the right to manage extends to the right to use surveillance in any way, shape or form. So even where there may be gaps in legislation or regulation, even with very large employers, there is a very strong view that the right to manage your workforce is your right, your decision to make alone, and that can use any kind of coercive technology.

The CHAIR: Thanks. Dylan.

Dylan WIGHT: Thank you. We have heard a bit of evidence around data that has been collected through surveillance being used for disciplinary procedures. Can you maybe just elaborate on how important it is that workers are given access to that data that is being collected on them, particularly in those instances or prior to those disciplinary procedures taking place?

Alana GINNIVAN: I can speak to that. In the submission we do provide context and significant detail on this, but an example that we would use of disciplinary action and surveillance being obtained is the use of body-worn cameras within a healthcare setting. This is internationally and nationally recognised as a deterrent to OVA against healthcare workers; there is an emerging body of research to support this. However, what it sheds light on is footage and information being captured during an individual receiving care—so they are in a vulnerable scenario, being in an inpatient, community or home setting, with footage being captured. What is occurring in a disciplinary measure is that excerpts of this, out of context, are being taken and transcribed as a snapshot. It does not consider the clinical element, the clinical decision-making required by nurses and midwives. It does not provide that. It will have perhaps a transcription of a sentence that somebody has stated from the scenario.

What that also reflects is that regarding this footage that is being regularly obtained, the question is: who owns the footage? Where is it being stored? In most cases this footage belongs to a private contractor. But what is happening is that registered practitioners—nurses and midwives—also face regulatory action by AHPRA and the national health board under health practitioner national law. So not only do we face potential disciplinary action at a local level, being your employer; that can extend to overarching governing bodies, being AHPRA, the CCYP, the Aged Care Quality and Safety Commission et cetera. So this footage, taken out of context, is being utilised in a punitive measure, and on top of that, employees and workers are not provided that footage in the first instance, because it does not belong to the healthcare provider. It is a private company's property, and they are not privy to how this footage is able to be stored, disseminated, destroyed et cetera.

Dylan WIGHT: But then the healthcare provider is able to get it off the—

Alana GINNIVAN: Not in all instances.

Dylan WIGHT: So you are saying that footage captured by body cam, which is there essentially to keep you safe from violence from somebody in a health setting, is being used in disciplinary procedures?

Alana GINNIVAN: Correct. And the other concern of that is the consent of the patients. It is sensitive information that is being obtained not only of the direct patient implicated; depending upon the scenario there are other patients, visitors, family. Who is in that footage? It is diverse, and the breadth is incredibly large. So it is occurring on a regular basis.

Dylan WIGHT: And for that to occur, there would be, for instance, a complaint, and then the health provider would have to go to the operator of the camera or whatever to obtain the footage?

Alana GINNIVAN: Yes, and they are not always afforded that in advance of disciplinary proceedings. They will not in all instances be provided that opportunity.

Dylan WIGHT: Sure.

Alysia BLACKHAM: Perhaps I can add to that. In preparing this submission the NTEU conducted a survey of its members and asked them about their experiences of surveillance and also how it was being used in the workplace. Some members reported that surveillance data had been used in performance proceedings and they were not actually aware that they were being surveilled in that way until disciplinary action was taken. To me, this seems like a real failure of due process and a real failure of transparency in the workplace. If you do not know how you are being tracked or surveilled and you do not know how you are being measured, it is an additional way of exerting control in the workplace. If you do not know what is happening, you are constantly concerned you are being surveilled, and that can affect workers' mental health, their wellbeing and also their feeling of security in the workplace. So I think these have broader issues.

Dylan WIGHT: Yes. Thank you.

Lauren KELLY: These same uses of surveillance are very common across our industries as well. Also, sometimes the uses of technology are quite banal and not particularly sophisticated at all. A very, very common grievance of our members across many industries is when there is a decision that has been made by management to terminate a particular worker. Then they go back to the CCTV footage, and they look at months of footage to find some kind of infraction, perhaps for time theft, which means being off task for several minutes, and then they use that to justify the termination that is already in the works. The same goes with body cam footage as well with our security workers and casino workers et cetera. Also, capturing conversations between workers—we have had workers disciplined for having organising conversations. Their level of surveillance is really at that personal level, capturing conversations between workers as well.

Libby MUIR: Libby Muir from ANMF. I am a Professional Officer as well. I think the other extension to what Alana is saying around context is often if we do not receive the footage in the lead-up to the disciplinary, we cannot give context to it. If you show it to the worker, often you will get, 'This was a situation that occurred around what I'm being brought before for the disciplinary.' Unless you have that information, you cannot represent the worker fairly and you cannot represent the situation. A lot of clinical scenarios, whether it be on CCTV or on body cam footage or whether it be an occupational violence or another situation, present in a certain way but have a lot of clinical context behind them that people do not understand and family may not understand.

Sarah ROBERTS: Sarah Roberts, Secretary of the Victorian Division of the NTEU. I think there is also a question here of notice. I think Alysia kind of referred to it. If you get advance notice of knowing that you are going to be surveilled, your behaviour might be different from what it might be if you are not getting that notice, especially when we are talking about surveillance in the home context. For people who are in our industry working from home, according to our survey, they suspect they are being surveilled, but they do not have any knowledge of it. So when that then is brought forward in a disciplinary context, there is an additional question of a failure to meet natural justice and procedural fairness, because those people have not ever been told that they are being surveilled, whether it is through camera or email or keystroke or whatever it might be. So there is that additional element too.

Alana GINNIVAN: Sorry, one further element to complement Sarah's comments around use of surveillance tracking when in the community. We have many members working across metro and regional Victoria going out into the community providing care. With the surveillance on vehicles that is used, when they understand that there is a presumption that they are being tracked per se, what we do see is that, from a KPI perspective, employers use this tracking data as a disciplinary to say, 'You're not meeting time targets,' when it does not factor in that the nurse has arrived and the patient is on the floor. There is all of this prolonged time to care that is not factored in, and these surveillance models are being used, and they can have extensive data on these members. They track it with their computer logging system of their notes. It is exhaustive, what they do provide, and it is being used in disciplinary matters, but it does not reflect the context of the clinical setting and in-home setting.

Anthony CIANFLONE: Thanks, Chair. Thank you all for appearing and all your respective members' fantastic work to help our community. I was actually fascinated, Alysia, by your opening remarks highlighting the fact that there is a gaping hole in current legislation in this space. In that context, you may be aware or may not be aware that the number one recommendation that has been put forward by the Victorian Chamber of Commerce and Industry, who appeared earlier today, is that:

> The Victorian Chamber believes that the existing legislative and regulatory framework is adequate and can be relied upon to address workplace harms arising from workplace surveillance.

I am curious to know what your response would be—and others, please feel free to jump in—to a position like that.

Alysia BLACKHAM: I would respectfully disagree. I have provided some additional evidence to the Committee which really lays out just how gaping these holes are, and we are seeing this repeatedly through the case law that is emerging. For example, in the federal jurisdiction there is case law where an employee computer—it was the computer issued by the employer—that entire computer, is seen as an employee record and therefore not subject to any privacy protection at the federal level, including personal passwords, health information, personal email. All of that is exempt from privacy and data protection law. And in Victoria, if they were working in the private sector, there would be no state-based protection either. To say that that is adequate regulation to me is not a true depiction of how things are working.

I think this has real consequences in practice. Employers may be inclined to do more and more surveillance, thinking that that is going to achieve better outcomes at work. But actually what we see is that it has more and more harms for workers and that employers are not getting the most from their workforce if they feel like they are being constantly surveilled in ways that are not clear or transparent. So I think this is having negative consequences for employers and for workers at the same time.

The law is not adequate, and we can see that if we look at other jurisdictions like the ACT or New South Wales, where they have put in place some measures to try to redress these gaps. That is not necessarily the full extent of regulation that we would recommend, but it gives an example of where the gaps really lie in Victoria.

Lauren KELLY: If I may add to that, I would completely agree with what you have said, and then it also has such a flow-on effect for unions in trying to respond to some of these issues when they arise for our members, because it is not as simple as saying to the employer, 'You're not allowed to do this.' Actually, the conversation becomes, 'You are allowed to do this, but you probably shouldn't.' That is a much more difficult campaign to run, and it means that rather than appealing to our industrial power, which is what we should be able to do as unions, we are often in a position where we have to run a public narrative campaign and say, 'Well, you can do this, but you shouldn't, and it's going to look bad for you if you do and it'll look bad to the public and it'll look bad to shareholders.' That is not what unions should be spending our time doing. We should be exercising our industrial strength, but in this domain we really do not have very much.

Anthony CIANFLONE: Just to pick up on that point as well, I note the survey results from NTEU's survey, which reported 29 per cent of employers use surveillance data for specific purposes. Sixty per cent were unsure about its main purpose, but overwhelmingly members reported that it was in relation to performance management, disciplinary actions, task allocation and monitoring and monitoring of union activity. So in that respect, I guess, talking to your submission: how can we improve the current legislation, a major piece of which was done back in 1999 for the surveillance Act? How can we modernise it for 2024?

Alysia BLACKHAM: Absolutely. In the NTEU submission we put forward a number of principles, which we recommend should inform that legal reform. In particular we need to move beyond a focus on data protection—that is important, but this is much bigger than just data protection. Really, we need to be thinking about substantive limits on when employers can or should surveil their workforce and in particular that that should be for a legitimate purpose and that it should be proportionate to that purpose. Actually, we need to be thinking about putting substantive limits on some of these technologies and how they are used and for what purpose, and that will lead to better outcomes for everyone at work.

Anthony CIANFLONE: Do you want to add to that?

Libby MUIR: Look, we would certainly also say that that legislation has not kept pace and we are seeing massive increases in surveillance, not only within the workplace by the employer but in the home and by family

and carers in the workplace. And because there is no legislation that outlines what both the consumer's and the employee's rights are—nurses' and midwives' rights are—they cannot stand up and say, 'Hang on a moment, please; you need to stop doing that.' So if they are in someone's home and that person decides that they are going to pull out their phone or they are going to set up a covert camera in the home and the nurse finds out about it, it is very difficult to confront that. There is nothing from their employer to say you have a right to actually say, 'No, thank you. We're not going to be doing that.' With legislation keeping pace with those sorts of scenarios and being structured properly, then we as a union can step forward and say, 'Where are your policies and procedures in relation to this?' so that the nurse or midwife knows what their obligations and their rights are but the consumer understands fully as well, because of the emotional distress, the psychological distress this is creating. Again, complementing what these guys are saying, you are going into an environment, you are providing personalised care—very personal care—and very time-critical care, and you do not know whether you are being videoed doing that, and if anything happens, how that will be construed and used is very stressful.

Anthony CIANFLONE: So the ANMF agree that the current legislation is outdated well and truly?

Libby MUIR: Well and truly.

Anthony CIANFLONE: Good to know.

Alana GINNIVAN: If I am just able to add to the comments, what it does demonstrate is that there is no consistent approach that is available to the breadth of the different industries to have a framework that underpins these policies and procedures. What is at play is that it is subjective to each organisation, each provider. What that means is it is highly discretionary and it leaves each worker, irrespective of the industry, at risk. By improving this legislation there is an opportunity to make this progressive and adapt it to what technologies are available and an opportunity to get abreast of what may be.

The CHAIR: Wayne.

Wayne FARNHAM: Thank you, Chair. Thank you all for coming in and for your submissions. I am going to lead into a few different things here, and I am glad you have come in because you are educating me as we go along, which is great. Just going back to Lauren, I think you said there was punitive surveillance, coercive surveillance, versus the right to manage. One part of this is where we find the balance in that, because I think that is very important. To be perfectly honest, I thought body cams were worn for your protection, so I am disappointed to find out they are being used in other avenues. That is quite disappointing. This is what I am trying to get to: where do we find the balance between your protection, your right to privacy, and the surveillance—all those things combined? How do you fix that? I know it is a pretty broad question, but as you are all at the work face of it, I am sure you have an opinion on it. Anyone can go first. I do not mind.

Alysia BLACKHAM: In terms of how we find the balance—and I think that is one of the really challenging questions in regulating this area—the first point is recognising that surveillance can have a legitimate role in terms of how we manage a workforce. It can be legitimate. It can be used legitimately if it is directed to a legitimate purpose and it is proportionate to that. On top of that, though, we need to recognise that even in the workplace workers have a right to privacy. The current legislation recognises that that exists in the bathroom, but I would say it also exists beyond the bathroom.

Wayne FARNHAM: A tearoom, for example?

Alysia BLACKHAM: The tearoom potentially in a discussion with your union delegate, or perhaps if you are accessing your private medical records at work or if you are corresponding with your spouse. These are things to me that form that critical privacy in the workplace, and this is something that has been acknowledged and respected and upheld in the law in the UK and in the EU. They recognise that even if you are at work, even if you are on a work device, you have a right to some degree of privacy as a worker, and we do not yet have that in Victoria or in Australia. So there is a balance to be struck. It needs to respect the right to privacy as in the Charter, and it needs to also respect that there are some uses that are legitimate but they need to be proportionate.

Lauren KELLY: If I may complicate matters a little bit further just to also point out that sometimes surveillance is not technologically mediated. It is very much organisationally embedded, and it looks different

across different industries. Just to give one example, my understanding is that Amazon does respect that there is no technological surveillance in the tearooms, but when we visit HR like to all take their lunch at that time and sit right next to the union official. No-one will make eye contact with the union when we go in, because all of HR and lawyers are sitting there having their lunch in the lunchroom as well. Also, our farm workers work and live really under the control of contractors. They live in dormitory arrangements. Often there is CCTV inside the home itself because it is considered an extension of the workplace. Their transport between the farm and the dormitory is provided by the contractor, so their movements are overseen day to day by people. Those kinds of forms of coercive control can creep up in ways that are very interpersonal and very intimate and not necessarily technologically sophisticated at all.

Alana GINNIVAN: To add to those comments, a way in which this could be improved is to take a risk assessment-based approach so there is an onus on the employer, irrespective of the industry, to undertake a risk assessment. It means that, again, it comes down to a consistent underpinning legislative framework that enables and empowers organisations and healthcare providers to have a framework to rely upon to then make sure that the intent and purpose of this surveillance is clear. It considers: what is the environment, what is the purpose and how is it going to be used, stored, disseminated et cetera? It then opens up the discussion and obligation with unions and makes it relevant and makes it transparent. I think, importantly, it is not to say that we do not support the surveillance. As we all agree, there is a place, but it is the balance. The purpose really of this discussion is: how can we make a tailored approach to a really broad issue? Having this underpinning framework with obligations would enable that.

Wayne FARNHAM: I just have a little follow-up there, and it is to do with consent, because it is one thing that has been brought up quite a bit in this inquiry. I am quite curious: do your employment contracts or anything have a consent clause to surveillance in them?

Alana GINNIVAN: No, and I think that is the problem again: it is discretionary. It is not an obligation to disclose the surveillance. That comes down to, again—in an ideal world if it was legislated it would become an obligation. It is about conveying to your employees what is being surveilled and how so that there is a true inferred consent that your employees are aware of. It is not just silent.

Alysia BLACKHAM: Can I build on that and maybe challenge the idea of consent as it applies at work. Employees are generally not in a position to decline consent, and if you have a clause put in your employment contract and you are offered the job on the condition that you consent to that, that is not true consent, because you are not going to turn down the job just because they said they might use CCTV in the workplace, for example. Particularly in the context of data protection law the idea of consent in the workplace has been really challenged in a lot of scholarship. It is not real consent; it is not meaningful consent. So it would be better to use something other than consent as our criteria to work out if something is legitimate.

Wayne FARNHAM: What would that be?

Alysia BLACKHAM: Again, in the NTEU's submission we put forward a number of principles that might guide that, but really we need legislative lines about what is acceptable and what is not. It is not up to the individual employee to consent or not, but actually it is about compliance with legislation and regulation that says that certain things are acceptable and certain things are not. Partly that is about is there a good reason for doing this and is it relevant to that reason, but partly also there are certain things we recommended in the submission that should not be allowed, like surveilling interactions with union officials, for example, so certain things that are just prohibited and cannot be consented to.

Wayne FARNHAM: Sure. Thank you.

Kim O'KEEFFE: Through the Chair.

The CHAIR: Sure.

Kim O'KEEFFE: Thank you. I am really interested. Obviously, there are some really valid reasons why we do need CCTV, particularly in the health sector when you get to emergency departments, you know, fairly volatile environments where they already have security in place. They would be logical examples that you would think no-one would dispute. I think this is the hard balance: when you have got staff that might be having a fairly broad role. For a few hours you might be down in emergency and then you might be up in a

different part, and you are feeling like you have actually given authority to that shift, for example, where you might be doing multiple things. I think this is the challenge when you have got that need to protect your staff and to make sure that people are well protected in the workplace but then you have also got the privacy of that person that needs to be considered. This is I think the thing we are all hearing, the to-and-fro—we have got quite a lot of people disputing workplace surveillance, we have got others saying, 'We must have this,' and we have got others saying nothing needs to change. These are some of the challenges, but your input is really valid. Thank you. Any comment on that in regard to having a valid reason?

Alysia BLACKHAM: Yes, and partly too it is about: well, what purposes do you put that CCTV to use for? You might use it to monitor customers, for example, or to monitor aggression in the workplace, but you do not then use it to track back employees' behaviour to monitor them for how many minutes they are in the bathroom, for example. So it may be that we allow certain forms of surveillance but we do not then allow them to be used in certain ways—for performance management, for example, or for excessive monitoring. There is a case in the UK, *Tilli v Whole Foods. Whole Foods* is a supermarket, and there they use CCTV. They told employees they use it to watch for theft, and then they used it to monitor her behaviour, her interaction with customers, timing her for every item she put through the checkout. In that case in the UK they said, 'Well, look, you can use it to watch customers, but you can't use it to watch her interactions with humans and to time them to the second.' So I think having that nuance in terms of how we use surveillance is really important.

Kim O'KEEFFE: And how that impacts on the actual staff as well.

Alysia BLACKHAM: Yes.

Libby MUIR: I think the other thing that came from our membership was the fact that the legislation and updating legislation would allow us then to be able to go to employers who have obligations to set policy and procedure around why they are surveilling, what it is used for and how it might then impact membership. It does actually also impede care, because if people are afraid to do things or to act fully to their clinical decision-making framework, they are less likely to provide care in a timely way. So it has significant impact. If the underpinning structure, as Alana and other people have said, is not there and the obligations on employers are not there, then people feel insecure, and it has ongoing and further ramifications for our membership because they can lose their registration.

The CHAIR: John.

John MULLAHY: Thank you all for being here in this very interesting panel discussion. This sort of leads on from that: why is it important for workplace surveillance to be considered a psychosocial hazard for work health and safety purposes, and what would it mean to your members?

Libby MUIR: Can you indulge me with a story about a member: new graduate, early career nurse, not a lot of experience, very aggressive family with a family member passing away in palliative care. So it was a highly emotionally charged scenario with lots of issues around pain and so on, and the family became a bit obsessed with this member. She went through a whole procedure. We had to get some legal support for her, and there was a lot of threat to her registration as well, although AHPRA saw no problem with her care. A little while later with another family, they were surveilling her, and so she was really insecure about what footage they might have taken. They also knew where she was. It was a regional area, so people knew people; they knew where she worked, they knew where she lived. She went on and stayed in palliative care and was really well supported by the ward, but another family then had a family member dying. They had family back in Greece. They wanted to take some footage to send back to Greece, so they just started videoing her. Because there are no policies and no underpinning procedures, she did not know what to do. So she went to her manager, the ANUM, on the shift. They did not know what to do; no-one knew what to do. No-one knew what was going to happen with the footage. Subsequently it was going to be put on Facebook. So her interaction with this person, who they thought was wonderful—they were actually doing it from a positive point of view—was potentially going to be put on Facebook, and this person, who had been through trauma and knew that this other family was still after her, was really psychologically impacted. It shook her confidence. She was thinking about leaving nursing. So for an example of how having a lack of boundaries around workplace surveillance and workers rights, we nearly—you know, we had to do a lot of work, and I still get calls from her. She is developing her career, but she was significantly shaken, to the point of wanting to leave the profession.

John MULLAHY: And we need our nurses; we definitely need our nurses.

Libby MUIR: We need early career nurses to stay in nursing.

John MULLAHY: Hundred per cent.

Libby MUIR: And she was a really highly respected graduate. They did a lot of work to try and help support her. But in a regional area you can easily be known by other people, and if she appeared on Facebook—there is a very short distance between people on Facebook, and that could have really led to comments on Facebook about her; it could have gone down a whole line. It was a good outcome. Because she had a relationship with the ANMF, we were able to get our occupational health and safety person to step in. The workplace then spoke to the family, and the family very kindly deleted the footage. But it is all circumstantial, and as Alana has been saying, it is really at the discretion of the workplace as to how they handle circumstances. The ramifications can be quite significant for our employees but also for the privacy of the person and the patients around that person where the footage has been taken, because it was a four-bed ward.

Alysia BLACKHAM: If I can add to that too. The psychosocial risks of surveillance are experienced unequally. Those who are more likely to experience stress, anxiety and psychosocial impacts are women, people who are from a non-white background and people who do not identify as heterosexual, so members of the queer community. They are more likely to experience the emotional and the psychosocial impacts of surveillance because they are less likely to feel like they fit the norm of the workplace. So the impacts here have equality impacts too, and they are more likely to lead to adverse outcomes for people who do not fit that normative idea of who the worker is.

Lauren KELLY: May I also add: we recently surveyed more than 500 warehouse distribution centre workers about a new really punitive over-the-top framework that a company has rolled out this year, and what we heard from hundreds and hundreds of workers is that this is affecting their mental health in really serious ways. People are talking about sitting in their car having panic attacks before going to work, being medicated because of the job, it causing marital problems and it causing breakdowns with their relationships with their children, which is really just heartbreaking to hear. And we have had—and I do not say this lightly—members talking about it making them feel suicidal, especially, to add to your point, cohorts of older men, who may find it hard to access mental health services, or there may be a certain stigma around that or they may feel that if they lose this job they do not have other employment opportunities. It really exacerbates that fear of losing your job. We have a lot of people talking about how dehumanising it is to be monitored second to second, to have their toilet breaks monitored, and just how they feel very resentful and often very ashamed. Sometimes they have worked for an employer for a very long time, and then they are being treated in this fashion in their workplace. And it is having a really big impact on their lives more broadly, not just in the workplace.

John MULLAHY: So the systemising of the monitoring: their workers are basically locked into what they have to do and they are being monitored full time, and if they do not hit their KPIs, then there will be consequences.

Lauren KELLY: At the moment for Woolworths DC workers, if they do not comply with 100 per cent of a particular speed-based metric, they can face disciplinary action. And it is applied with discretion, so—

John MULLAHY: So it is up to the manager or whoever as to how they want to enforce it.

Lauren KELLY: Yes. but it affects everyone, because you know that you could be targeted for any reason.

John MULLAHY: Thank you.

The CHAIR: I want to touch on—we have not talked about it a lot today, but we have in other hearings and submissions—biometric data. Can you maybe give some examples of where you are seeing it being used? I see that you have some suggestions about it—that it should be an opt-in scenario for that biometric data. I would just like to invite you to talk about that, your thoughts. Is anyone collecting fingerprints—blood, I am assuming, maybe, in the health setting?

Alana GINNIVAN: Yes. The biometric data of fingerprints and retina scans and the storage—depending upon your role you can be required to have invasive blood-screening checks if you are in an immunocompromised area or you are in corrections. As a nurse, as a minimum, or a midwife, you have to have a certain level of immunity to be able to be permitted to work, given the high-risk nature. So once again, it comes to light that it is not clear to the employees the storage and the distribution of this data.

The CHAIR: And who owns the data.

Alana GINNIVAN: Correct, yes.

The CHAIR: And how it is being used then later.

Alana GINNIVAN: Yes.

Alysia BLACKHAM: And to that we can add the data flows. Often companies are outsourcing the collection, the management, the storage and the analysis of this data, and it is often flowing to four or five different companies, and employees are not notified as to where their data is going. This is not something we have seen yet in the higher education sector, but certainly biometric data is sensitive data. It should be treated with the utmost care, and there should be clear clarity around where the data is going or restrictions on where it goes, and that is not currently the case.

The CHAIR: Okay. Thank you. Kim.

Kim O'KEEFFE: Thank you. It is very interesting. We could stay here lots of the day. Some of your submissions mentioned the need for an independent body to oversee workplace surveillance. What powers and responsibilities do you think this body should have?

Alysia BLACKHAM: One of the key things in terms of how we task this body is they should have the capacity to investigate compliance and have strong powers to escalate that in cases of noncompliance. Bodies like the Fair Work Ombudsman provide a really nice model of the powers that can be given to a workplace inspectorate body. They do have powers to escalate in cases of noncompliance. So that might be one model in terms of the powers that that body is given. We provide some other suggestions in our submission too in terms of how that body could be structured. The key, though, is ensuring they have enough resourcing to do the job properly. There is no use in setting up a new body that then does not have the funding to do the job really well.

Kim O'KEEFFE: Anyone else?

Lauren KELLY: If I can just also add, all of us are speaking about pretty unionised industries, some really powerful industries, so our members are actually unique and an anomaly in the Australian broader workforce landscape. I guess I am just highlighting that policies and procedures and a strong union to enforce them—that is an experience of work that is unfortunately pretty unique in Australia. So I guess just also raising the point that for a lot of workers perhaps having something in the national employment standards to just capture workplaces that are not covered by enterprise agreements and unions, which is so many workplaces—because I think actually what we are hearing is when a workplace is quite strong and is quite unionised, employers have to be quite sophisticated in their ways of disciplining the workforce. You do not have to be particularly sophisticated at all if you have a workforce with much less systemic power; you can really just do whatever you like.

Kim O'KEEFFE: And the other thing that has been raised has been all the different industries that obviously are going to be impacted by this, and I am always interested in small business because I had a small business myself. How do they manage this change of legislation? What support is needed to do that? And that is probably a big issue with this perception of 'What does this mean to me? What does this look like within my business?' I have been talking to quite a few people in regard to this—the hearings that we are having—and we were talking about workplace safety, and it has been really interesting some of the comments coming back. A lot of it has been quite concerning. They are concerned—some of the businesses are very concerned about, 'How am I going to be able to manage this? Am I going to be able to afford this?' What does this look like, particularly in small business?

Alysia BLACKHAM: I would anticipate though that small businesses often are run more informally and they are less reliant on these sorts of technological surveillance mechanisms because you are seeing everyone in the workplace every day and you can manage people in that interpersonal way, which often gets lost in a large organisation. So I would say perhaps small business will be less affected by changes in this area and this is more likely to impact larger employers where they are managing large workforces and trying to do that at scale using technology and relying on quantitative metrics rather than that interpersonal relationship.

Kim O'KEEFFE: Depending on the costing, if this is fairly streamlined, what does that look like to a smaller business that does not have the financial capacity or may struggle with that? Thank you.

The CHAIR: Thank you. Dylan.

Dylan WIGHT: Thank you. I was just interested in talking about whether the respective unions have begun trying to bargain this into agreements, how successful that has been and what the limitations are to that compared to legislation.

Alysia BLACKHAM: I can speak to a study that I performed looking at enterprise agreements across the country, and I have provided the Committee with that write-up. Essentially it is very rare for provisions on this topic to make it into an enterprise agreement. There are many other things on the bargaining table, and this is not always the priority. Industries where this has made it into an enterprise agreement are often in the mining sector, and then often it relates to things around drug testing onsite, essentially, and how do they manage that process. So these are highly unionised workplaces with very particular needs. Otherwise this has not really been addressed in bargaining, and where it has been there is no legislative backbone or standard against which these clauses are being determined.

Dylan WIGHT: No safety net to it, yes.

Alysia BLACKHAM: They might be fairly open-ended. They do not necessarily provide substantive rights to workers in a way that we might like to see in legislation. There is no normative standard to back it.

Sarah ROBERTS: And can I add to that, I know the ACTU is developing model clauses around workplace surveillance for the purposes of bargaining and so on. But really if that is to evolve into the bargaining sphere, whether that ends up finally in collective workplace agreements is ultimately a test of the density of the relevant union in that area. So strong unions—my colleagues here—will be able to achieve those sorts of outcomes, but where we have less density and where that does not as a result rise to the top of the agenda, then you will not see that so much. For the places where we are less unionised there will not be those outcomes, so that is why there is more of a need for there to be governmental intervention.

Dylan WIGHT: And we are seeing less EBAs, particularly in the private sector year on year anyway, and very few of them in small business, which is already exempt from this. So I guess the whole crux of it is that underpinning legislation is essential, even if you can improve that through bargaining.

Sarah ROBERTS: Yes.

The CHAIR: Anthony.

Anthony CIANFLONE: Thanks, Chair. Look, my question is around artificial intelligence. I think it is agreed that there is a big gap in current legislation. But in terms of AI coming on the horizon, I guess question 1 is: what do you anticipate the impacts to be, and are currently being, given it is in its infancy and evolving quickly? And number 2: what regulation should the Victorian Government look at potentially through this inquiry to put some safeguards around it, as the Chair refers to, to help place workers and a balance of business interests at the centre of that as humans?

Alysia BLACKHAM: AI makes this incredibly important to deal with properly, because data is the new commodity, right? These systems are being trained on huge amounts of data, and that could potentially be workers data. That would then mean surveillance systems are gathering data that is then being used to train AI-based systems or being onsold to third parties to train their AI-based systems. One of the real concerns we have put forward in our submission is that there is no restriction on employers onselling workers' data for a profit and commoditising it in that way, which is a major gap in the regulatory framework. The incentives to create

datasets and onsell them for various uses are growing, and this is really important to be addressed in a proactive way.

Anthony CIANFLONE: Do you have any examples, by any chance, of cases where AI-procured data has been onsold? Are we aware of any cases?

Alysia BLACKHAM: I am not aware of any cases off the top of my head. One of the real challenges in this area is that there is very little transparency about what is being gathered and how it is being used. We do have cases where data has been transferred across multiple companies, not necessarily for sale.

Anthony CIANFLONE: And without the consent of the workers from which that data was derived.

Alysia BLACKHAM: Yes, that is correct.

Alana GINNIVAN: We would agree with the comments of lack of transparency. The other issue with AI—I should not say issue; element—is that it is a probability-based model. It does not understand the data. It does not contemplate, from our members' experience, data obtained within a clinical healthcare setting. The risks are, when this workplace surveillance is obtained and improperly used, for the data that was obtained for workplace surveillance the intent was not for AI modelling. The Office of the Australian Information Commissioner has recently released guidelines on it, and it is very clear about the risks surrounding personal and sensitive information. And within a healthcare setting that is all footage captured. And this impacts—again, it is not just about the workers; this is healthcare consumers. This is each and every one of us that can be directly impacted by this because, in the instance that this data is obtained in a meta scoop, if you will—I do not know if that is the correct terminology, but I am going to go with it—then you have no control as an employee, a worker, of this data that is now out in the metaverse. You cannot have it removed. You do not know how it is being perpetuated, and you do not know where it is. So the risk not only to the worker but the patients, again bringing it back to the healthcare setting, is profound. And there are no safeguarding provisions. There are no obligations on employers as it stands with respect to process and policy. What is being considered with this data that is being obtained? So with respect to health care, it is incredibly problematic. Obviously there are learnings—AI is the way of the future; we do see that—but there are no obligations and safeguarding in place to protect the workers or the patients and consumers.

The CHAIR: You talked about AI and onselling, but there is a risk of, obviously, hacking as well with this.

Alysia BLACKHAM: Yes, absolutely.

The CHAIR: Have you seen any of that, or have you got a case to point to with that?

Alysia BLACKHAM: There have been repeated hacks. One of the examples that I put forward in my paper is that if it was customers data that was hacked, privacy law would cover it and there would be penalties, but if it is workers data that is hacked, privacy law does not cover it and there are no penalties. So it is a very strange inconsistency in terms of how the law works right now.

One of the other things that was put forward in our members survey that we report in the submission was a real concern for academics around lecture recordings. Lecture recordings are the new way of educating. Many universities see them as a fantastic innovation, but that is a really valuable dataset, and there are real concerns that while they have been recorded to educate students, they might then be turned into other forms of data and turned into other forms of value, essentially, undermining education.

John MULLAHY: Or that video being able to be used instead of someone being in the classroom.

Alysia BLACKHAM: And there have been a number of examples where people have left or passed away and their lectures are still being used.

Alana GINNIVAN: Another element to the AI modelling is if the information is incorrect. It is difficult to determine the generated information—it appears as correct and valid. What another element of these guidelines did highlight with respect to marginalised populations is that, because it cannot determine between underpinning bias that is within the information that is obtained, it then runs the risk of projecting and perpetuating these marginalised populations with this information that is obtained. Again, in the instance of

Medicare being hacked, all of that information—that information of diagnosis, history—is available and can be used, and it is not clear where this is all going.

Lauren KELLY: I will just add as well: much more banal uses of algorithms in terms of algorithmic decision-making are a really big issue for our members, and it often looks like certain HR functions to algorithms are being outsourced—rostering software, other kinds of clocking in and out and also sometimes directions being fed to workers on the floor as to how to do the job and how long it should take et cetera. Some of those management functions are being outsourced to algorithms and digital devices, which raises a whole host of issues, but it can also sometimes be used as a way for management to hide behind the things they are doing. It is way of saying, 'Well, the decision has been made by the computer.' It is this very bureaucratic kind of 'computer says no' or 'computer says "not fast enough"'. So it has whole layers of complexity that I think really seek to obscure the responsibility of employers to their workers and really erode any sense of mutual reciprocity as well. It puts this artificial barrier between communications or different sorts of management processes between managers and their workers as well, and a lot of workers report it just being very frustrating. Their shifts can change last minute; they are expected to be clocking into these various apps and things and checking where they should be on a particular day. It is often changing, and often their directions for work are being fed via headsets, digital devices and the like. So it can have a very atomising effect on the experience of work as well and can feel quite dehumanising after long periods of time too.

The CHAIR: Interesting. Thanks. Wayne.

Wayne FARNHAM: Thank you, Chair. We have had a couple of conversations. We have leaned in today about the ACT and New South Wales having already started their reforms, and there are federal reforms going on at the moment. I assume it is just an assumption that you talk to your interstate colleagues. What they are saying to you from interstate—is there a positive improvement in what New South Wales and the ACT are doing? But also, do you think we should be taking a federal approach, or a harmonised approach, to this across the country so we do not have cross-border differences between ACT and New South Wales or New South Wales and Victoria? What are your thoughts on that?

Alysia BLACKHAM: I cannot speak to the experiences of my colleagues interstate. But in terms of adopting a harmonised approach across the country, I think it is really critical that we regulate sooner rather than later, and a harmonised approach will take time. It is perhaps something to aspire to longer term. It may reduce the regulatory cost for business if we could adopt a harmonised approach, but it will take too long in a context where technology is changing really quickly and employees experiences are being affected right now. I would recommend Victoria take the lead, make a change and then seek harmonisation later.

Sarah ROBERTS: I can report, in terms of communication with interstate colleagues from New South Wales and the ACT when we conducted our survey about this—and that was reported at our national executive level—that there was a general consensus, including amongst those people, that this was still widely and deeply felt across the community, continuing in New South Wales and the ACT. I do not have any insights to say that as a result of the legislation things are fixed there.

Wayne FARNHAM: Have they improved?

Sarah ROBERTS: Well, it would be wrong of me to say that there had been that conversation, but there was just a general sense in the room that these problems that were being highlighted by members of ours in Victoria were the same in New South Wales and the ACT, especially around not knowing about whether surveillance was going on. But I would endorse Alysia's comments: I think harmonisation is obviously something that would be desirable.

Alana GINNIVAN: We have commonalities obviously with the other states, and so from member experiences in New South Wales and ACT, they have the experiences of devices—of personal devices—being used to obtain footage from workers, as we have discussed at length today. But what they do have is the underpinning obligations within the Act that they are required to consult. They need to provide notice in advance of the implementation of these surveillance devices, they have to describe what the intent is, so it provides the opportunity. Again, it is about raising the education and the awareness of what is being surveilled, and then there is a dispute option. There is also the option that there is regulatory action for the misuse of this information, so it provides a framework again that all employers are aware of.

The other unique element that we do have is we have members on the border of New South Wales and Victoria. They are employed by, for example, Albury Wodonga Health, and they can fall under the auspice of two jurisdictions. It is a unique scenario, and we do have members across the cross-border that are subject to the differing legislation.

Wayne FARNHAM: Thank you.

The CHAIR: John, I reckon we have got time for one more.

Wayne FARNHAM: Excellent. Some of your submissions argue that the workplace surveillance leads to function creep and work intensification. Can you give us some examples of what impacts these effects have on members—your workers?

Lauren KELLY: Absolutely. I can think of dozens of examples across industries, but I think the logic of it is pretty consistent across the board, which is that when you have a work environment that is very technologically mediated and also a managerial style that is quite low trust and authoritarian, it results in a situation where people feel like every second, every minute, of work is being quantified and being tallied up against some kind of KPI. It can create a lot of unsafe work practices, with people working too fast in environments that are really dangerous. Logistics is just one example, but there are many. It can have serious flow-on effects in terms of harm.

There are also environments in which people are working very closely with automation now, and there is an argument to be made that the machine is setting the pace of work and people are trying to keep up with that, particularly in distribution. Depending on the employer often and the style of management, you really can have a case where people feel like they are working like robots and with robots in some ways, rather than the promise of automation and all of these glorious technologies, which was that we would continue to be the brain and the machine would do all the heavy, dirty, dark lifting work. But often what we find in these environments is a lot of the creative or executive function or the decision-making is outsourced to machines, and you just have the very dexterous workers running around, breaking their backs trying to carry heavy things and keep up with machines. So I think the promise of automation and a lot of these technologies has not come to fruition, and then when you have that in an environment where people are being so closely scrutinised minute to minute, it makes it not only a really unenjoyable but potentially very dangerous work environment as well.

Alysia BLACKHAM: In terms of professional work, we are seeing the introduction of keystroke software that monitors how many keystrokes you make every minute, every second, every hour, and how many hours you are at your computer every day. This poses really significant risks of injury.

The CHAIR: I am laughing because it is unbelievable, isn't it?

Alysia BLACKHAM: Yes. We are likely to see a growth in occupational injuries if people are expected to remain at a computer continuously for this time. We also have members reporting that they have been told that they are not on Teams long enough, that they need to log into Teams every day to report that they are there, ready for work, then log out so they know when they have gone, or that they are having their bathroom breaks. So their breaks are being monitored.

Certainly this is breeding intensification of work. It also does not recognise the diversity of work. Particularly coming from an academic setting, we do work on paper, then on the computer, then we talk on the phone, but if you are just monitoring keystrokes it is not reflecting the diversity of tasks that someone would do on a given day.

John MULLAHY: Can they pick up how quickly you are reading something? Is that the next step?

Alysia BLACKHAM: Not that I am aware of yet.

Lauren KELLY: If I can just make the point—I think it is sort of obvious but may be worth just making explicit—that these uses of surveillance do not do anything for productivity or efficiency. They create a range of perverse outcomes that are often very time consuming. We often hear from employers, 'We need these things to remain competitive and ensure productivity, efficiency et cetera,' but actually it often creates barriers

to people just getting on and doing their work. So it really is a mechanism of control; it is really not linked to efficiency or productivity.

Alysia BLACKHAM: One example of that is that Microsoft Teams will give you a prompt to say that you have not sent as many emails as your colleagues. Arguably if you are sending more emails, you are less productive because you have not resolved the issue quickly, but it is an example of the perverse incentives.

Wayne FARNHAM: So do you just jump on email and go 'Send', 'Send', 'Send' to all your contacts?

Alysia BLACKHAM: Fortunately my institution has not activated that setting, so I have no idea how many emails I send compared to my colleagues.

The CHAIR: Thank you so much. I think we could keep chatting all afternoon, but thank you so much for your time, your submissions and all the work that you are doing. We appreciate you taking our questions today as well.

Witnesses withdrew.