T R A N S C R I P T

LEGISLATIVE ASSEMBLY ECONOMY AND INFRASTRUCTURE COMMITTEE

Inquiry into workplace surveillance

Melbourne – Tuesday 3 September 2024

MEMBERS

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

WITNESSES

Leroy Lazaro, Victorian Branch Secretary, Postal and Telecommunication Branch, and

Troy McGuinness, Elected Organiser, Postal and Telecommunication Branch, Communication Workers Union;

Karen Batt, Secretary, Victorian Branch, and

Jason Cleeland, Manager, Membership and Information Technology, Victorian Branch, Community and Public Sector Union;

Tash Wark, Secretary, Victorian and Tasmanian Authorities and Services Branch,

Simon Hammersley, Research and Policy Adviser, Victorian and Tasmanian Authorities and Services Branch,

Laura Boehm, Industrial Officer, Victorian Private Sector Branch, and

Kat Hardy, Lead Organiser, Victorian Private Sector Branch, Australian Services Union; and

Nicole McPherson, National Assistant Secretary, and

Matthew Rowe, National Executive Member, Finance Sector Union.

The CHAIR: Welcome, panel, to the 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.

Now, we are going to run this session straight into a sort of a Q and A format. Committee members will ask some questions. If you wish to answer that particular question, you can raise your hand and we will come to you. Just to make it easier and clear for our Hansard reporters to document our hearing today, could you state your name and the organisation or union that you are from. There might not be an opportunity for everyone to answer every question, so depending on time we will just see how we go. But if it is a burning one that you would like to do, please shoot your hand up straightaway and we will allow two or three speakers to answer each question before moving on. If there are, though, some points that you think that you have not had an opportunity to speak to, you are more than welcome to provide additional information in writing after today.

We will quickly introduce ourselves as the Committee and then we will just jump straight into some questions. Thank you, and thank you for your time today. I am Alison, the Chair and Member for Bellarine.

Kim O'KEEFFE: I am Kim O'Keefe, Deputy Chair and Member for Shepparton. Welcome.

Anthony CIANFLONE: I am Anthony Cianflone, the Member for Pascoe Vale.

John MULLAHY: John Mullahy, Member for Glen Waverley.

Dylan WIGHT: Dylan Wight, Member for Tarneit.

The CHAIR: I am just going to get myself sorted. Kim, we might go to you first if that is okay.

Kim O'KEEFFE: Yes, sure. Thank you so much. Welcome, everyone; it is actually a very impressive panel we have got in front of us now. My question is: at what point does workplace surveillance become excessive, and could you give some examples?

The CHAIR: Who would like to jump in first?

Kim O'KEEFFE: Is that a tough question?

The CHAIR: Thank you so much. If you could just state your name and where you are from, thank you.

Kat HARDY: Kat Hardy, Australian Services Union, private sector branch. There are certainly a variety of different examples that I think we could give as to where workplace surveillance has been used excessively, but I think the broad point that we come to with this is that the question—and this is not a reflection on that question specifically, it is how it is always discussed—comes at it from the wrong direction. It is not necessarily at what point has workplace surveillance crossed the line, or at least it should not be. It should be: when is workplace surveillance actually necessary, and that is when it is implemented, not the other way around. The starting point should be: is this necessary for processes, for security, for worker safety? If so, let us look at what we can implement, rather than workplace surveillance is okay up until the point that it crosses this line here.

Examples of where it is over the line are certainly when it is monitoring people on an individual basis for micromanagement, looking at people's specific word choices rather than doing broad coaching; when it gets into the use for micromanagement of employees rather than improving processes or improving service quality; and when it is tracking people, particularly when they are not working. There are a whole range of areas and examples that I am sure all the unions could give where it crosses the line. But the starting point I think is: we have to look at 'is it necessary before it is implemented' rather than 'do we roll it back once it crosses the line?'

The CHAIR: Thank you.

Karen BATT: Karen Batt from the Community and Public Sector Union. I concur with that, but I also think parts of the areas that we are grappling with at the moment relate to issues around what happens and what is recorded in their private time, particularly in that crossover between working from home and working from the office, and issues associated with, say, Microsoft 365, which has keystroke monitoring in it. There are no guidelines, no real clear guardrails, if you like, for the rolling out of this in workplaces at the moment in Victoria. I think, similar to my colleague at the end, that we need to have a very clear view as to why it is necessary, what the purpose of it is, where the data is being stored, why it is being stored and how it is going to be used. Without that, it can be pretty much a free-for-all.

The CHAIR: Thank you. Tash.

Tash WARK: Tash Wark from the Australian Services Union. I concur with everything that both Kat and Karen have said. I guess it is also that we know that this is a problem now, that there is excessive monitoring happening now. As preparation for this we surveyed a whole bunch of our members from across our coverage. Our members are from local government, public sector agencies and the community sector—so a really wide range of different kinds of groups. They are being monitored now at home, as others have said. Their social media is being monitored and that kind of stuff, and there is really nothing to protect that. That is a really big problem from our point of view. The other thing that I do not think others have touched on yet, and I am sure others will, is just the lack of awareness about whether people are being monitored. I think our members feel really unsure about what is actually in place. I think that is a massive problem. There needs to be certainty about 'Is my employer actually watching what I do?' and 'How are they watching it?' as well as where data is being kept and if it is even necessary in the first place, because we know what is happening now is beyond.

The CHAIR: Thank you. Anthony.

Anthony CIANFLONE: Thanks, Chair. Thank you all for coming in, for all your respective submissions and for all the work you do to represent workers across Victoria. Thank you. We heard some other evidence earlier on today around gaps in the current legislation in Victoria, obviously what has happened legislation-wise in New South Wales and the ACT and a review that is happening federally in the privacy space. There has also been as part of that discussion some talk about potential new regulatory bodies or an oversight body being introduced in Victoria in terms of how workplace surveillance is implemented in different workplaces, whether in government or non-government spaces, whether there is a role for WorkSafe potentially from a workplace health and safety perspective and whether there is a role as well for the office of the Victorian information and privacy commissioner from an access to data point of view. I am just keen to get your respective thoughts from a union perspective around whether there is scope for that space to be better regulated and have better oversight than currently is the case on behalf of members.

Laura BOEHM: Thank you. If it is possible, I would like to just refer to the first part of your question, which was about bringing in legislation in light of the fact that there is a Commonwealth review of the *Privacy Act*. Our position is it is very necessary to have specific state legislation on workplace privacy, like New South Wales has and like the ACT has. That is because it is not a sure thing that the *Privacy Act* is considered a workplace law under the *Fair Work Act*. The *Fair Work Act* under section 12 requires a workplace law to be something that regulates the relationship between employees and employers. We know that the *Privacy Act* is incredibly broad. It is not a sure thing that the review will even have it dealing with workplace privacy issues. If we create state legislation that goes to workplace privacy, it will very likely be a workplace law for the purposes of the *Fair Work Act*, which can then create additional protections for employees in Victoria who ask questions about the protections that they have under that legislation. It is also important because then there will be able to be I guess a fairer process through disciplinary processes up to and including dismissals.

The CHAIR: Thank you, Laura. Would anyone else like to speak to that?

Karen BATT: Yes, I would. Karen Batt, CPSU. We think that whilst WorkSafe Victoria does not yet define this sort of surveillance or AI usage as a workplace psychosocial hazard, we actually think there is space for WorkSafe to do some work in this area. We have also done a survey. It is a big group and we all do the same survey. Responses that we got were about making them feel small and making them feel they were not trusted. That then feeds into a workplace culture that can become toxic, and that has a big impact on someone's psychosocial health. So we think, yes, there is a space. It does need to be regulated. And as I said, we need guardrails for this. It is too much of a free-for-all at the moment.

The CHAIR: Any thought on that oversight body, though—there has been talk about that today—of who or how that could be implemented?

Laura BOEHM: I guess a point, I suppose, in our submission that we have mentioned is the fact that it should be a created body. I do not think that it is necessarily the case that it cannot be WorkSafe. I think that part of the attraction of using WorkSafe is that WorkSafe is used to mediating disputes between employers and employee representatives as well as employees. One really fantastic thing that has been brought up repeatedly throughout today has been the need for consultation. One part of the *Occupational Health and Safety Act* that is quite impressive and that WorkSafe already has experience in doing is the consultation and negotiation requirements for designated work groups, so when there is creation of these DWGs, WorkSafe can come in to resolve legitimate disputes between employees and employers.

Part of our submissions and a lot of submissions is that we should be having meaningful consultation, which includes, in our opinion, negotiation that can be accommodated, and has been accommodated, by state legislation before under the *Occupational Health and Safety Act*, so maybe WorkSafe is well placed to play that role.

Nicole McPHERSON: Nicole McPherson from the Finance Sector Union. One of the biggest challenges that we see in the finance sector is that there is already almost complete surveillance of our members across the sector, and it has been that way for the best part of a decade. There are existing obligations on employers to consult with workers on risk assessments to identify hazards. We know that surveillance is a hazard, and there is currently no consultation whatsoever. So the existing regulatory regime is simply ineffective in in any way addressing the fact that there are health and safety implications of workplace surveillance. We think there is also potential that there should be consultation from an industrial perspective on the introduction of workplace surveillance, that it enlivens the consultation obligations. I see my friend has got the *Fair Work Act* here, in case we all need to look at it, but I will not be doing that personally.

We are not seeing consultation from a health and safety perspective; we are not seeing consultation from an industrial perspective. We are not seeing consultation in any way, shape or form, and that gives us real concern that the existing regulatory options that we have and that should be happening at the moment are not effective in dealing with this enormously increased, I guess, technological environment that we are dealing with now.

Anthony CIANFLONE: That is in a bit of contrast to some of the evidence we heard earlier from the Business Council of Australia representative –

Nicole McPHERSON: I do not doubt that.

Anthony CIANFLONE: and I would even presume some of their members would be organisations whose workers you represent.

Nicole McPHERSON: There certainly are, yes.

Anthony CIANFLONE: Are you aware within the banking sector or the finance sector of any of those respective banks or financial institutions actually proactively consulting with staff to any extent about implementation or ongoing rollout of surveillance technology in the workplace? Are you aware of any?

Nicole McPHERSON: I am aware that none of them are. The only organisation that has proactively consulted with the union is AustralianSuper, and they have done very good, thorough consultation. One of the really concerning parts for us when it comes to workplace surveillance is we often find out that the surveillance is happening when one of our members falls foul of the requirements somehow and it comes up as part of a disciplinary process. That is when we find out the surveillance was happening and that is when the workers find out the surveillance was happening. Quite often we also find out from, for example, our friends at the business council, who proudly talk about how, you know, BCA members are using AI in a particular way. We find out from their public statements. So currently I would say it is fair to say that across the vast majority of the finance sector—so across the banks, across the insurance and across the superannuation funds—there is no transparency whatsoever on what surveillance is being used, how it is being used, how the data is recorded, whether it is disposed of at any point in time. Workers simply do not know what tools are being used, and the only way they find out is when the data gained through that surveillance is used in some kind of adverse way.

Anthony CIANFLONE: And through that process, even then is there any opportunity to extract further insights on behalf of your member or worker in the process of that dispute for their information and your broader information, or is that still very tightly held on to by the –

Nicole McPHERSON: Very rarely, because usually what happens is the employer tells us that the evidence that they have got is proprietary or otherwise confidential and it simply cannot be disclosed. I know this is in the questions that are to come, but another one of the elements of this that we are seeing is that the surveillance that workers are subject to produces an enormous amount of data. It used to be the case that in order for that data to be used it needed to be processed by a human being, and there were natural limitations on how many human beings you could find to process that data. But with the increasing use of AI, which can crunch this data in a very quick way, what we are now seeing is that conclusions are being drawn from the data gained from workplace surveillance that are frequently incorrect or misrepresent the situation, but AI overlaid with the workplace surveillance has really created a monster that is happening in a completely unregulated space.

John MULLAHY: I would like to drill down a little bit further into that. In the FSU's submission it mentions that AI is used to analyse workers' sentiment towards customers or their employer.

Nicole McPHERSON: Yes.

John MULLAHY: How common is the practice in the industries you represent, and can you give some examples? And then following on from that, what are the dangers of sentiment analysis?

Nicole McPHERSON: Thank you for the question. One of the biggest problems with the sentiment analysis and how widespread it is is that we do not know, because employers do not tell us when they are using these technologies; they do not tell workers when they are using these technologies. They do not disclose it at all to anybody, so we simply do not know. The employers that we know that are using sentiment analysis we know because it has been disclosed to us through the course of disciplinary procedures against our members. That is how we find out, and then we of course go back and try to get further information on how widespread the use is. But even from our disciplinary process work we do know that it is being used to assess interactions with customers, either on chat—so when you might use a chatbot to contact your bank, on the contact centre, financial advisers are being monitored in that way. But what we are also starting to see is that it is also analysing sentiment in communications between workers, and that is where we have a really significant concern, in the chilling effect that workplace surveillance can have on the ability for workers to have democracy in the workplace.

John MULLAHY: But a specific example of what has led to some disciplinary action from this analysis, like this AI—can you give us something specific?

Nicole McPHERSON: Absolutely. We refer to a couple in our submission, but I am happy to go through those again. One of them was one ne of our members was having a conversation—they are a financial adviser for one of the big employers in our sector—with a member of their organisation. Building rapport at the start of the conversation they said, 'Unfortunately it's been really rainy lately,' and the overall sentiment of that conversation was marked as a sad face, and that was because when we went back and drilled down into what the issue was with the conversation—otherwise it was a very positive, productive conversation—it was because they had used the word 'unfortunately'. That triggered the AI to say there is actually a problem here and the sentiment of the conversation is a negative one. Of course, when we sat down as part of a disciplinary process and listened to that recording, it was very clear that there was no sentiment problem with that conversation at all. But the enormous issue with that, or one of the enormous issues with that, is that it means that there is a disciplinary process that one of our members is subject to, and we all know the enormous stress of being involved in a disciplinary process; even if it ultimately turns into nothing, it is still a really difficult thing to go through. And we also know that a lot of workers who might not have the benefit of being a union member unfortunately go into that situation on their own; they do not know that they can ask for the recording, and they often just cop the consequence even if it is entirely unfair.

Jason CLEELAND: Jason Cleeland from the CPSU. Just in relation to what you were talking about and the knowledge that there might be surveillance going on, listening to conversations and things like that, one of the issues that our members have raised in our survey on the use of AI in the public sector was that there are a lot of tools that get installed and implemented in businesses that the business does not even know at the time has this

sort of surveillance and recording technology going on. They might only find that out later on, when it becomes useful for them to be able to use in procedures against employees. I think that sort of leads into where the regulatory environment is important, because there really needs to be some focus at the moment, with the implementation of all of these sorts of tools: there are things that surveil workers without even the employer knowing that it happens, and so people really need to pay some attention to it. I think that sort of thing is going to become increasingly likely with things like Copilot and Recall from Microsoft that will sit there monitoring an employee's own desktop and workplace and all of the emails that they send. It would be very useful for them in their day-to-day work, but where is that information being stored, and who else has access to be able to watch it?

Nicole McPHERSON: Could I just make one very brief comment? We had a manager bragging to us that they could go in and do a word search for 'union' and see which of their staff were talking to each other about the union and respond accordingly.

Dylan WIGHT: Yes, I was going to speak on that. There are obviously some issues around disciplinary procedures and how surveillance is being used in respect to that. We have spoken at length about the ACT and New South Wales, their legislation and aligning more with that. As part of their legislation, it is prohibited to interfere with I guess employees' capacity to engage in the industrial space. Does everyone have examples of surveillance being used that way by employers to disincentivise being active within your union or participating in industrial relations within your workplace?

Laura BOEHM: Very recently we had a workplace where there was the first union paid meeting at the worksite, and it was clear that they were using CCTV data to tell people, 'You were 5 minutes late back to your desk,' letting them know that they knew who was attending the union meeting and that they were being closely watched.

John MULLAHY: Anyone else got any examples of that?

Kat HARDY: Kat Hardy, ASU private sector. I know the ACT legislation references not preventing union communications in the workplace, but we have certainly have examples of employers where if a member has their workplace email as their contact with us, they suddenly stop receiving union communications, and it turns out that, oh, no-one has heard from us in a couple of months unless we have got their personal email. I have certainly seen that as well.

Nicole McPHERSON: We have that happen all the time. There are certain employers that are notorious for it. What we see the impact is workers self-regulating their own behaviour. When they know that all of their Teams messages, all of their emails are being watched by their employer, they adjust their own behaviour to not engage in behaviours that might fall foul of Big Brother. And it is particularly an issue in our sector because we have so many of our members working from home, so the only option they have to engage with each other is via digital channels. They do not have the option to go and have a site meeting. It is just simply not an option, especially with national employers, where their team might be across the country. Getting them all in a room is not a possibility, so when they have to engage via digital channels and all of the digital channels are monitored all of the time, it has a naturally chilling effect on their ability and their willingness to talk to each other about industrial issues at work.

John MULLAHY: And that is why WhatsApp and Signal are quite useful to your members.

Nicole McPHERSON: Absolutely. And I will say probably 90 per cent of our union communication now happens on channels outside of the workplace. But then there is also a reluctance in some workers to use those, because they do not necessarily trust them.

Dylan WIGHT: Can I just ask—and it is certainly for the benefit of me but I would say probably most of the panel—if there was specific legislation in Victoria that covered that and prohibited that sort of activity, does it then have the capacity to intersect with the *Fair Work Act* so you can actually go and prosecute these claims in the commission? Do you know what I mean?

Karen BATT: Karen Batt, CPSU. It would need to be very clearly articulated how it sits in terms of Victorian law and the referral power to the Commonwealth to make sure that it is not something that has not been referred, because then the *Fair Work Act* does not have the jurisdiction. So you would need to do quite a

bit of I suppose that clinical work with the Commonwealth around: is it captured by the *Fair Work Act*? What is the gap within Victoria for that to be covered?

Dylan WIGHT: We spoke about this earlier to the law institute here. I mean, there will be oversight of whatever legislation there may be in the future, whether that is a new independent oversight, whether it goes into OVIC, wherever it goes. But then it is no good just stopping there—and I do not think a good outcome for workers is then going to the Magistrates' Court, for instance. So it is more just advice—if this were to be something in the future, how do we do it so it intersects properly with the *Fair Work Act* so it is then prosecutable in the commission?

Karen BATT: Well, it would need advice from Industrial Relations Victoria to this panel or to whoever is drafting the legislation to say whether the referral power that already exists has picked up this emerging issue in a workplace. If it has, then it is covered, and they would need to tell you how, but if it is a gap in the referral and Victoria has not referred it, the *Fair Work Act* has no jurisdiction. So it would need to be a bit of research work around that constitutional question.

Dylan WIGHT: Great, thank you.

The CHAIR: Laura, yes.

Laura BOEHM: We all know that there are already restrictions on adverse action towards people for being part of a union, you know, advocating on behalf of unions. All of those protections do already exist under the *Fair Work Act* and under our own *Equal Opportunity Act* as well regarding union activity, but I think the real value of the surveillance legislation, state-based legislation, is trying to penalise the prohibited use or use of surveillance data outside the scope that is hopefully negotiated with employee input. Whether or not that gets taken through the Fair Work Commission or whether that is instead just through WorkSafe or whatever does not seem to be the biggest issue.

Karen BATT: May I add a supplement? There is also the question of the Victorian code of conduct for the public sector and the public service that has a direct interface with behaviours in workplaces, in particular the areas around monitoring of social media and public comment. So that would also need to be factored into what sort of expanse you want it to have for the purposes of coverage of the *Fair Work Act*.

Dylan WIGHT: Okay.

The CHAIR: Thank you.

Kim O'KEEFFE: How can the Victorian Government ensure that workers are giving genuine consent to workplace surveillance?

The CHAIR: Thanks. Laura.

Laura BOEHM: In our submissions we make it clear that we are against blanket consent clauses being allowed under contracts. It is so commonly the case that we will get members who suddenly are in a disciplinary process where they are getting an IT audit in order to beef up the charges against them, and we will look into their contract and see there is a blanket clause saying you agree to 'any and all surveillance that we come up with'. We are totally against that. If there are new technologies coming in, that needs to start a fresh set of consultation with the employees or the affected employees.

Karen BATT: Karen Batt. We have also had some issues regarding implied consent in relation to telematics in cars and the monitoring of data of where people are going, where they are stopping and how long they are stopping for and then that being somehow used for disciplinary purposes, particularly if they have taken unexplained more than 5-minute stops on a particular road. That then starts to feed into disciplinary matters within some government departments that use this data. I think there are issues around that that also need to be factored in. It should not be an implied consent because you are taking a government car. It should be explained to you what the telematics are within the car, where the information is going, how it is going to be used and what it is not going to be used for. We have had a number of disputes with a couple of departments around the misuse of data collected by telematics coming into a disciplinary matter. Yet it was someone who had been ill

and had stopped a number of times for various needs, and that had not been picked up by the AI and the data—but we had to go through a disciplinary process to manage that.

Leroy LAZARO: Just to speak a bit more on the topic, even though managers or management tell staff that itis going to be used for certain purposes, they actually do not. They go over and above that to use it for other purposes. So if our workers are on the road delivering mail, if they are being monitored through telematics and basically doing their job in a very safe matter at the speed limits they are supposed to, then the management's view is it is taking them too long to do the job, so they are monitored and put through disciplinary processes and sometimes recommended to be dismissed. That is where we have to go and battle that, take it off and put the person back. But the anxiety and stress it has caused the person through that three- or four-week period, not having an income in some cases or sitting at home and not doing anything—it causes another problem for them and their families.

Tash WARK: Tash again, from the ASU. About 40 per cent of our members said that they were not aware of whether they are being surveilled or not. It comes back to it cannot just be a hidden line in a contract or a policy that you sign on that first day when you are kind of thrust with probably a whole lot of links to a data piece somewhere. It really needs to be overt to people—'This is what is happening; this is the relevance of it as well'—what the actual reason is for using those measures and then where that information is going. Who sees it? I mean, we have had some really creepy examples over the year of managers who will just sit in a room watching the telematics screen or watching the call centre clocking over and not in a constructive way. I think you can have all the systems in the world and then still things just go wrong apparently. It needs to be super clear to people.

The CHAIR: Thank you. Anthony.

Anthony CIANFLONE: Thank you. Can perhaps each of you talk to an example of how through an EBA process an employer may have potentially tried to embed provisions in their interest in relation to workplace surveillance as part of an agreement, whether overtly being open and transparent with unions about that or not, and also, on the other side of the coin, examples of where unions or worker representatives may have through an EBA process tried to identify, highlight, prevent, install or include workplace surveillance-type measures within an agreement in the interests of workers. For example—just a bit of context—we had the information commission here earlier. They gave a mature example of how they have installed CCTV cameras throughout their premises in the context of the sensitive information that they deal with every day on behalf of the Victorian Government through cabinet documents and the like, where they have strict processes around where two people from management have to be able to access and review footage only on a certain criteria basis. So they are very clear and transparent it appears in terms of the protocols around that. But from your end: what is your experience with employers seeking to embed or being open about embedding surveillance through the negotiation process?

Tash WARK: Tash from the ASU, Authorities and Services—sorry, I forgot to specify my branch before. It is a really common one that comes up a lot in local government bargaining tools to a degree and some of the public sector bargaining we do. I would say that in terms of the kinds of claims that employers are putting forward it is about them having open slather on disciplinary matters. You can just imagine that we put forward claims that say disciplinary matters will be carved out: information will not be collected, stored et cetera for the purposes of any disciplinary matters. If it is about safety, because usually it is about safety or it is about asset protection, that those things are real, and then the flow-on measures, if it is genuinely about safety or asset protection, can be about driving behaviour. I have had that in a community sector bargain where we got really, really stuck on GPS because they really wanted to make sure people were driving safely, and therefore they thought that there needed to be a clause in the agreement that also provided for disciplinary outcomes if people were found not to drive safely, through monitoring driving behaviour. That is not going to fix that problem, and it is probably going to make people really, really anxious. So I think our plans are always about trying to have transparency and consultation—that there is clarity about the kind of data being collected and what the purpose is, that it aligns with the purpose, who has access to it, and that it is destroyed after a period. If you want to genuinely address some of those things, then it is engaging with workers in an open kind of way rather than trying to make it punitive.

Karen BATT: I was just going to say that we have also had some discussions around enterprise agreements in this space. We actually found out that it was initially rolled out in certain programs in government—I am

talking about GPS telematics, around the safety and security component. It is not until after they roll it out that you have to then wind it back, because it is not just about the security of where a particular van might be, but it is also they switch on the audio in the cars and listen to someone chatting. They then have a whole range of things because there are not any restrictions around it. So it has to be case by case. My staff have to go in and negotiate it and put restrictions around the use of what is collected in the cars through the telematics and GPS so it cannot be used in discipline purposes. But it is always reactionary. There is no formal obligation, because the departments think they are doing the right thing in a safety and security measure. But the reality is, because of what data is collected and what is available to be used and no frameworks around it, we have got this problem that emerges day after day.

The CHAIR: And the technology is just advancing so quickly ahead of –

Karen BATT: When you add that to the AI, and the generative AI that has come about in the last two years, it is a phenomenally fast-moving space that I think has workers quite frightened, but no-one really knows who to turn to.

Anthony CIANFLONE: That is the point I was getting to, Chair, as well—we have a *Surveillance Devices Act* in Victoria that is really pre-internet days. It is not being captured through any of the EBA processes, so it is almost another layer of opportunity for the imposition of surveillance devices on workers without any scrutiny or real oversight.

Karen BATT: Absolutely.

Nicole McPHERSON: I am happy to respond to this as well. Nicole McPherson from the Finance Sector Union. One of the reasons that we spend so long talking about surveillance and AI in enterprise agreement bargaining processes is because the regulatory environment is absent, so if we want any kind of control in this area we are forced to use enterprise bargaining agreements to create some kind of regulatory framework. That is not a fabulous situation to be in for a range of reasons, but it is where we are. In our sector we bargain about 100 enterprise agreements, so we have a high bargaining load. I do not recall ever seeing an employer trying to put surveillance clauses into an enterprise agreement, and I think there are probably two reasons for that. One is that the finance sector is very highly regulated, and my suspicion would be that employers pretty much do whatever surveillance they want and use the fig leaf of the higher regulatory environment to do that. My other idea would be that they have contract rights to do this kind of surveillance, so they do not really need an enterprise agreement clause to enable them to do it. We always put clauses on the table in bargaining processes to limit the amount of surveillance that can happen on workers and also to contain how AI can be used in the workplace. We are having increasing success with those clauses now. We recently negotiated the first full suite of those clauses that limits the amount of surveillance that can happen, requires disclosure, provides additional consultation if a role is displaced because of AI—really a very modern clause, but that is the very first one in our sector, and we have a lot more work to do in that space.

Troy McGUINNESS: Troy McGuinness from the Communication Workers Union. We mainly cover Australia Post and Telstra and they are national, so we do not really have this come up with EBA stuff, but what we do find with both of these companies is they are very HR driven. Therefore they go off to HR and they get HR to draft themselves up a policy which does not really get shared out to the wider workforce, so they do not understand what the policy is. They do not understand what the policy entails. We generally get told that these things are going to be put in (1) for the workers' safety and (2) for security. That is when they first implement it, and now we are five or six years down the road, more and more it gets used for discipline purposes. I have had many conversations with senior managers saying, 'Well, how is it that this has come about? Why are we even looking at it? You were meant to be investigating this.' They go, 'Well, when we were investigating it and we looked through it, we saw stuff that we couldn't unsee, so now we have to address that.' When you read the wording of your policy, you are meant to use this as a tool to be able to educate workers, let them know that they have done something unsafe and this is where they need to try and address safety and give them the opportunity to rectify the situation or change their behaviours. But no, what we find more and more nowadays is they look at the telematics for reasons they are not meant to be looking at them for, and then they are putting our members straight on a disciplinary inquiry and then using HR to back them up, to try and dismiss people for basically just going about the same job that they have done for the last 25 or 30 years. So this is where it is a very big issue.

The CHAIR: Thank you. John.

John MULLAHY: A lot of you have members that are in New South Wales and the ACT. We have been discussing the actual legislation in those jurisdictions and what we can do here in Victoria. In those jurisdictions do they actually have access to any of their surveillance data from the organisations, and if so, why would it be important for workers to have the right to access the data collected on them through surveillance?

Nicole McPHERSON: We are a federal union. I can respond to that. I am not aware of any of my members in New South Wales or the ACT being told that they can access their data. That does not surprise me, because why would an employer do such a thing? I suspect that there is not a great deal of knowledge about particular state laws, so I would suspect that workers are not asking. But there has certainly been no groundswell of workers requesting their information. Why is it important? I think it is critically important to take a small step back for people to know how they are being surveilled, what kind of information is being collected and then that they can access that information. At the moment people do not even know what kind of surveillance is happening. What we tell our members is: 'You should assume that every moment at work is recorded in some fashion, because it basically is in some way, shape or form.' Basically every single moment is recorded in some fashion.

The point my colleague made earlier I think is a really good one. There are a whole range of tools now that Microsoft rolls out that have surveillance capabilities that even employers do not know about. Microsoft Viva has a whole range of surveillance functions. If anyone has done a Zoom meeting lately, there is an AI button that has a whole range of new things that you can do. These technologies are happening more quickly than technology teams and employers can train people to use the tools. The pace of it is extraordinary, and we understand to some degree why the regulation has trailed the technology, because I do not think any regulatory regime could possibly keep pace with this. But to us that means that the urgency around this is just growing day by day. This is a crisis in the finance sector, and we need to do something immediately about it.

John MULLAHY: If there is disciplinary action, are you able to get all the data, or are they just presenting you with some evidence on the issue at hand?

Nicole McPHERSON: Just the evidence on the issue at hand, and even when we specifically request the information or request the system through which that information was gained, we are not given that, because we are always told that it is proprietary or confidential. When we ask what that means, we are not able to find that out. Of course any decision that involves AI decision-making all happens in black box decision-making ways, and even the employers do not often know how that decision was made.

John MULLAHY: Computer says no.

Nicole McPHERSON: Yes, computer says no, and nobody will ever find out the actual answer.

Laura BOEHM: Just to jump off that point about the lack of disclosure that the employers provide when there is a disciplinary process on foot, that is absolutely our experience. It is forever frustrating. We also have employers who will just hold the idea that they have got data that they may or may not have against our employees. I have had circumstances where it is like 'If you continue pushing, how about we just do a bit of a search on your phone records?' or 'I've got CCTV footage?' 'Can we see it?' 'No, you can't.' An issue is the asymmetry of information and the sword of Damocles hanging above our heads, whether that is going to be used against us and suddenly we will have to grapple with things that we had no idea we were up against. Like Troy was saying earlier, you go in for one thing, and through the process of trying to establish the employer's claim against an employee they will bring up all sorts of things that they were not originally looking for.

I think there is a question that we were primed to think about before coming here, which was about disciplinary processes and about unfair dismissal. An additional reason from a legal perspective about why it is so important that there is a balancing of the information available to people during the disciplinary process is because we know that if this goes to the Fair Work Commission for an unfair dismissal, for example, the valid reason does not have to be the information that the employer had at the time the dismissal occurred. That can come later. They can do an IT audit and provide that as additional evidence for poor performance, and then suddenly we are scrambling. That is a really common experience. Like you said, Nicole, you are giving employees the primer: 'Hey, just so you're aware, you may be recorded in a million different ways.' That is not a healthy and safe thing for us to be telling our members: always watch your back.

Nicole McPHERSON: Can I just make one additional comment to that. One of the biggest frustrations that we have is that when one of our members, for example, makes a bullying complaint against their employer and there might be surveillance evidence that we know would support their claim, workers cannot access this data. We know the data exists—everybody knows that it exists—but workers cannot access it where it will support their claim. Only employers can access it where it will support their claim. So in terms of information asymmetry it is a scandal.

Dylan WIGHT: On top of that, we heard earlier today that accessing this information through FOI requests is quite complex. It is hard to get around some of the exemptions. As we heard, it is being consistently used in disciplinary processes and workers do not have a right to access their own data. What does best practice in respect to this look like?

Karen BATT: Karen Batt from CPSU. We do access the CCTV footage, particularly in areas like use of force in the prisons. We are able to access it to ascertain: was it really use of force or was there something else? So that aspect of it is open for us, and I think that the way that is handled allows us to look at the processes associated with a disciplinary matter inside those facilities. What we find difficult, which is a bit more of the black box aspect in discipline, is we do not know what the coding is. We do not know what the inherent biases are within that coding, and so someone may be picked up for not being at work on a Friday consistently even though they are paid to be there. They have got a requirement to be there, but the data does not record them. But it also does not record the fact that they might be going to the synagogue or to the mosque because that is their religious day. So we have quite a lot of that black box thinking and the application of that to day-to-day working environments that we have to unpick each time we deal with a disciplinary matter.

The CHAIR: Karen, did you want to add any more to the other question?

Karen BATT: No, I just added that on to that one.

The CHAIR: Thank you. We got to you. Dylan, do you have any further questions?

Dylan WIGHT: No, I just want to reiterate that obviously it is a clear issue that workers do not have access to their own data. What does that fundamental change look like?

Kat HARDY: Kat Hardy, ASU. I think that there are a range of things that need to be in place around data that include what it is for, how it is stored and for how long that I think are part of that best practice. Knowing from the beginning who will be able to access it—workers should have access to it—but also what elements of it they will be able to access: there should be able to be a consultation and a negotiation process around what elements of this workers will be able to access on implementation. At this point in so many industries it is too late but starting afresh. There are so many areas—unpaid overtime, for example—when we come to collectively bargain, looking at workloads, all of these things, where this data could be very useful in shifting some of the balance of power that has been lost through the use of surveillance that we currently cannot access. So having a very clear and negotiated understanding as to what the workers will be able to access I think is essential, as well as how decisions will be made using the data that is collected. Yes, as to what was flagged earlier: what are the underlying assumptions that are made in these programs? But also, when someone is flagged through AI as not having met KPIs, has a person actually reviewed that before someone is brought before a disciplinary proceeding? Has that been checked to see, 'Oh actually on that day they were, for example, acting as a delegate and that is why they weren't at their desk.' Has that actually been reviewed against their performance by a manager or someone with some professional expertise? I think that is the other important part of the use of data that needs to be laid out at the start in these processes too.

Dylan WIGHT: Is there scope for workers to have to have been given access to data that is going to be subject to a disciplinary meeting? Do you know what I mean? If you are walking into a disciplinary meeting and you are talking about something that you have potentially done wrong at work and you have had absolutely no access to the data that is being used for that, I would think that both as a worker and potentially as a representative of that worker you are at a pretty distinct disadvantage.

Karen BATT: It is a breach of natural justice. The underpinning principle of all of our enterprise agreements is that a worker must be afforded natural justice in a disciplinary setting or in an underperformance setting. If you have information that is only held by one party to that, that is a denial of natural justice. So I think that needs to be one of the principles we also look at this legislation through.

Tash WARK: I think just the same information needs to be provided to everybody. If it is data that is about a worker, they should be able to see it. I would like to be able to say that when human beings are involved it is better, but it is not always. I think we have got examples, particularly in depot environments, where workers are often timed about what time they get back to the yard. We have had members who have gone through disciplinary processes because a manager kind of clocks them as half an hour late, but actually they have been out the back greasing blades or that kind of stuff. There just needs to be a little bit more common sense about going and asking the question before you put someone through a really crappy process because you think you have got information on your side—just some kind of rigour around, 'Okay. Here's the information, but have I actually just gone and explored that a little bit before I start persecuting people?'

Laura BOEHM: Just to jump off a couple of things that have been raised about the black box decision-making—I know it is not answering your question directly, so apologies, but it has been raised about the black box decision-making and the importance of having a human involved in the decision-making. That is really important for general protections under the *Fair Work Act*, and our general protections have been flogged for so long to a point where they are becoming very unhelpful for workers. The worst thing would be to not have protections against there being an employer relying upon what the computer says, as you put it earlier, because in order for general protections to work you need an identified decision-maker and you need to be able to put yourself in the shoes of the decision-maker and say what was in their mind. If what was in their mind was, 'I do what the computer tells me,' it has made general protections extremely weak, and general protections are sometimes the only thing some people have. So it is really important that we do not allow that to happen.

Tash WARK: Contracting it out to a computer.

Nicole McPHERSON: Our view on when AI is—and I know this is not the subject of this inquiry, but our view on that, for what it is worth, is that where AI is being used in a dismissal there should be the inference that the dismissal was done for the prohibited reason unless it can be displaced. We think that that onus needs to be flipped when it comes to general protections, which is Commonwealth law. While I am talking, I might just answer your question. When it comes to the regulatory environment that we think needs to exist in workplace surveillance, we think there does need to be a reset. I think that is a really important thing that needs to happen in our sector. We think that starting from the position of there being a prohibition on workplace surveillance is a sensible place to start, with then carve-outs as exceptions for where it is required, and for us the exceptions should be where it is genuinely required to comply with regulatory requirements and where it is genuinely required to promote or protect worker health and safety. We can imagine a situation where it might be required to support process improvements, for example, but for us they should be the only three exceptions to a prohibition on workplace surveillance.

Karen BATT: Could I also just add that it is incredibly important that we have from our sector a whole-of-government policy setting because at the moment there is the likelihood that agencies may do their own, and so if we talk about the public service itself, it is 55 agencies. Then you have got the sector itself. If government as an employer wants to be a leader entity, the whole process needs to have a very constructed set of policy frameworks around it so everyone knows what the rules are and it cannot be varied between agency and agency.

Anthony CIANFLONE: Just picking up on that point, for example, generally speaking, when a worker starts a new role or is trained up or upskilled to another role in an organisation, whether government or non-government, there is usually some sort of onboarding kit where there are a set of expectations that are placed in the kit around workplace OH&S—whether it is around a code of conduct, for example. Expectations essentially in that pack usually—and I am generalising here—are from an employer in terms of their expectations of that worker. Is there scope or opportunity for consideration by the Committee to be given to some sort of pledge potentially around workplace surveillance or disclosure of workplace surveillance from an employer to an employee as part of some sort of kit that employees usually receive as part of any onboarding or upskilling?

Karen BATT: The only thing I would say about that is that we need something that is enforceable. The enforceability of practices is essential for us to enforce workplace rights. If it is, you know, 'I pledge to be a nice person and let you know what data there is'—that is not necessarily going to work. So I do think you might have it as part of a new starters kit, but if there is not some teeth behind it, the problems we are all dealing with will just continue to exacerbate, even worse, as AI starts to grow exponentially.

Anthony CIANFLONE: Yes. Whether it is mandatory or not, I am more making the point around: there is always expectation put on a worker when they come in by an employer. Potentially there is scope for them as employers to be fully disclosing about how they are monitoring the conduct—again whether it is legal or otherwise.

Simon HAMMERSLEY: Simon Hammersley at the Australian Services Union, Authorities and Services Branch. The disclosure needs to be ongoing too because this is a space that is changing very quickly. So a one-off when you start a job could never be enough to cover what is happening in workplaces now.

Dylan WIGHT: That is what I was going to say. The overwhelming evidence has been that disclosure is not enough. It needs to be genuine and ongoing consultation.

The CHAIR: Thank you. I am just mindful of time, so what I want to do—and this is very dangerous of me—is open it up. Is there anything we have not covered, that we have not asked today, that you would really like to press upon the Committee?

Karen BATT: May I say one thing?

The CHAIR: Yes.

Karen BATT: We absolutely 100 per cent support the Trades Hall submission about a Privacy in Working Life Act. Victoria could lead the way, and it would be fantastic if this committee made that recommendation.

The CHAIR: Okay. Thank you.

Kat HARDY: I absolutely agree with that as well. I might just highlight another reason why this is so important that this happens: it is about the rights around people and how we protect them when disciplinary action happens. It is also about how people feel about their work and the impact that has on workers as human beings. If they feel constantly under surveillance or mistrusted, they will stop taking work or helping people if they are meeting their stats, or they cannot talk about anything because of fear of being overheard or listened to. That grinds people down on a day-to-day basis. It makes working life worse and it drastically shifts the balance of power. This is really essential that this happens, to actually improve the quality of life for all working Victorians. I think that the Privacy in Working Life Act is necessary, because we are talking about in many areas marginalised workers who do not always have access to a union to support them. In many ways the people who are we are talking about are the best-case scenario because at least they have that support. I think that is really essential for shifting this balance.

Leroy LAZARO: I forgot to introduce myself before—Leroy is my name. I think workplace surveillance should be used for educating, for safety and security, and not be used as a tool to dismiss or discipline people. If there is some act of violence or other sort of thing, that is a different situation. But performance and behaviour—it should not be used to discipline or dismiss employees. In fact it should be used in a different method, what it is really meant for: to protect the products or for the safety of people and to correct behaviour. That is exactly what it should be used for.

Kim O'KEEFFE: I just might comment in regard to your point about really making sure that we understand the mental health aspects of what is happening in their workplace, and people respond to that differently, so we need to make sure that there is something in place to address that. Because you are absolutely right—this is the impact it is having. Some people will be quite stressed about being under surveillance, whether it is for good or bad reasons, while others may manage that really well. So how do we deal with those staffers that are actually impacted personally with their mental health? I think that is a really big point.

Laura BOEHM: Following on from that point that was made earlier about remote workers who feel like they cannot reach out to colleagues to have those important discussions in the workplace, and who do not have those connections—eight hours of the day being spent glued to the screen trying to not step out of line is a really miserable day.

The CHAIR: Thank you for your submissions. Thank you for appearing today and thank you for all the work that you are doing in providing us with some evidence today. If there is anything further, though, you

would like to provide, something that has come up today that you think you would like to add, you can always submit that to us in writing as well. So we appreciate it, again, and thank you for your time.

Witnesses withdrew.