T R A N S C R I P T

LEGISLATIVE ASSEMBLY ECONOMY AND INFRASTRUCTURE COMMITTEE

Inquiry into workplace surveillance

East Melbourne – Thursday 26 September 2024

(via videoconference)

MEMBERS

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

WITNESS

Adjunct Professor Moira Paterson, Castan Centre for Human Rights Law, Faculty of Law, Monash University.

The CHAIR: Welcome to the public hearings for the Legislative Assembly Economy and Infrastructure Committee's Inquiry into workplace surveillance. All mobile telephones should now be turned to silent.

All evidence given today is being recorded by Hansard and broadcast live on the Parliament's website. While all evidence taken by the Committee is protected by parliamentary privilege, comments repeated outside of this hearing, including on social media, may not be protected by this privilege.

Witnesses will be provided with a proof version of the transcript to check. Verified transcripts and other documents provided to the Committee during the hearing will be published on the Committee's website.

I will just remind members and witnesses to mute their microphones when not speaking just to minimise that interference.

Thank you so much, Moira, for joining us today and taking some of our questions. We have had a big day of all different perspectives and I am sure we have got lots of great questions for you as well. I thought, though, we might start with giving you a few minutes just to give us either a bit of background or a little bit of information to help us start, and then we will head over to some committee members to ask you some questions.

Moira PATERSON: Sure. Good afternoon and thank you very much for the invitation to speak to you. I am here representing the Castan Centre for Human Rights Law at Monash University based on my expertise in the area of privacy and data protection law. It is my submission to you that the law in Victoria currently provides inadequate protection of workers' privacy and that this is a worsening issue in light of the increased scope and proliferation of surveillance in the workplace in an era of big data and artificial intelligence. So it is our view that there need to be some new or amended surveillance law and also ideally some updating of the data protection regime in Victoria. I think I will leave it at that so you can ask some questions.

The CHAIR: Yes, perfect. That is fine, and it is probably best that we go into questions, because we get a little bit more out of the questions as well. Dylan, I might go to you first to ask the first question.

Dylan WIGHT: Thank you, Chair. Thank you, Moira, for appearing today. We have seen in several submissions and also heard from a mountain of evidence that the genuine consent model to workplace surveillance is problematic and probably inadequate due to an innate power imbalance within the workplace between employers and employees. What is the best way to inform—that might not be the right word. What is the best way to introduce workplace surveillance, or the best framework to introduce workplace surveillance, in respect to consulting your workers, and also what other legal protections could Victoria set up to overcome that issue?

Moira PATERSON: That is quite a big question, but in terms of what employers can do, I think part of the answer to privacy issues, strangely, is transparency. That does not overcome the consent problem, but particularly when you have surveillance that people are not aware of, or they are not aware of the parameters of it, and even more especially once you bring in AI, then there is a whole lot of—I am sure if you have heard of the concept of the black box. The problem with AI is there is a very poor understanding of how it operates. In terms of legal protection, there is not a lot, partly because there is a big hole in the Commonwealth Privacy Act for workplace privacy. In terms of Victoria, you have got the Privacy and Data Protection Act, and that does apply in the public sector, but it is not fully up to date on larger technological developments, which is why you will have, I am sure, read in some of the submissions about the GDPR and some of the advantages of that. But really if you cannot protect people through consent, then what you can do, in addition to requiring consent and informing them about what is happening, is to bring in some sorts of tests of necessity and proportionality, and that is really one of the important things that does. The problem is, though, that that still leaves the private sector. As I said, the Commonwealth Privacy Act notionally protects the private sector. It does not do so in respect of employment records, and it has also got a big hole in terms of the small business sector, which is basically something like 90 per cent notionally of the bodies that might be covered.

So that is where you come to surveillance law. Victoria has got the Surveillance Devices Act, but that does not work for a number of reasons. It does have workplace provisions, but they are confined to toilets and bathrooms and that sort of thing. It really does not provide very effective protection in terms of, say, listening. It deals with listening devices, optical surveillance devices and tracking devices, which sounds pretty good. The problem with the listening devices is that it applies only in respect to private conversations, being a conversation carried

on in circumstances that might reasonably be taken to indicate the parties to it desire to be heard only by themselves and ought reasonably not to expect it to be overheard by others, which does not cover a lot of what happens in a workplace. For optical surveillance it is even worse because it only applies outside buildings and is also subject to a similar restriction. For tracking devices it only applies in relation to devices that are designed solely for tracking, and a lot of the tracking devices are multidimensional. For data surveillance devices it only applies to law enforcement and does not apply to anyone else. So that means you have got a law that applies across the board but it really does not provide optimal protection to anyone, and that is also the case with employees.

As you are aware, there are a couple of specific sui generis workplace surveillance laws in the ACT and New South Wales. Again, I would not suggest modelling on those, because they seem to rely on consent. They do not bring in tests of proportionality and necessity and so forth, but that is another way of trying to deal with this. Also there is beefing up the provisions within the Surveillance Devices Act, because your Privacy and Data Protection Act is not going to cover what you need, I do not think, at this stage. Although there is the Privacy Act federally, it is not dealing with things like employee records or the small business exemption. I am not sure if that fully answers what you wanted, Dylan.

Dylan WIGHT: No, that is fine. Thank you.

The CHAIR: Thank you, Moira. Kim, I will go to you next for the next question.

Kim O'KEEFFE: Sure. Thank you. Thank you for joining us, Moira. It is really great to have you here, and thank you so much for the submission. There are a lot of interesting facts and data and things in there. I just thought one of the interesting things I have come across is that some of the submissions have recommended the creation of an independent body to oversee workplace surveillance and deal with complaints. Should there be one body to oversee the act of surveillance and another to deal with the data collected, or could one body do both?

Moira PATERSON: To my mind it would be more efficient to give it to OVIC given that they have got the expertise in that area, and it is quite a complex area. But I would say that is subject to one really big proviso, and that is that they get funded for it. They are very stretched at the moment, and if you give them a new function, then all that does is undermine their ability to protect other aspects. To my mind it makes sense. I know there are perhaps some issues that might be unique to workplaces, but a lot of what they do involves considering specific contexts, so I think they are certainly well equipped to do that.

Kim O'KEEFFE: Thanks.

The CHAIR: Thank you. Anthony.

Anthony CIANFLONE: Thanks, Chair. And thank you so much, Moira, for being here. My question is around better ensuring fairness when it comes to workplace surveillance and data collection. Picking up from what Dylan was asking you about earlier on: on top of consent, what protections could the Victorian Government set up to ensure workplace surveillance is more reasonable and better proportionate to reflect the interests and wellbeing of workers? We have heard a lot from the employer side today from a couple of different contributions and submissions, but prior to that we heard even more from workers and union representatives about how disproportionate and unfair, from their perspective, current laws and arrangements are, because they frankly rely a lot on the good faith of employers working with employees. What is your view around how we can better get the balance right?

Moira PATERSON: Gosh, that is a difficult question. I think that it comes back to the core principles. When you are looking at stuff like proportionality and necessity, if one goes through the process, then you start to unpack why it is necessary. There are a number of legitimate reasons why employers might want or need to engage in data collection and surveillance in specific circumstances, but what is often the case is that what is collected goes beyond that—way beyond that, number one. But it is not necessarily then used just for that purpose, or there is no guarantee that is just used; as you say, it is just a question of trust. There is no requirement to keep it secure, so you are creating a pool of information that is potentially of interest to other people. If it is not kept secure there is a risk of hacking.

There is certainly now money in collecting information, particularly with AI, for training data. There are all these possibilities, and so while not denying there may be appropriate reasons for data collection or surveillance, it is a question of narrowing it and saying you only collect what is necessary. You need to demonstrate that. How you are going about it needs to be—how does that impact on the employee's rights, and is there a less intrusive way of collecting that information? And then once you have got it, what safeguards do you have in place and what guarantees do they have that that is not being misused? And then even further down the track, with AI, we are moving to an area where a lot of decisions are being automated, like recruitment and all sorts of things—promotions. So now this data is being collected, it is being used for automated decision-making. There is a lot of concern and evidence that automated decision-making is only as good as the programming and only as good as the training data that is fed into it. So it is quite possible, and there have certainly been many examples documented, where there is bias. Sometimes it is because of the way the program is set up, but more likely because of the training data.

Essentially you have to feed the machine lots of examples so that it learns. Sometimes data about specific groups is lacking, just historically or whatever, and so that means it may be less accurate in respect to them. It may mean that it discriminates, not from any deliberate programming but just because that has happened. What is happening there, as I say, is happening in a so-called black box, because even the people who design that decision-making software themselves would have difficulty explaining how it arrives at a particular decision, because a lot of the modern automated decision-making relies on the machine itself learning and changing as more and more data is fed into it, so it is not just putting in a simple equation and then getting it to act on that. There might be that at the beginning, but then the machine goes off in directions using neural networks and so forth, and that means that you have got very important decisions affecting individuals being made in a way that is difficult to explain. I can well understand that if you are an employee whether or not you get promoted, or for a potential employee whether you get employed, and all sorts of other things—assessments about your performance—if these things are all automated, there can be a lot of unfairness there.

I just point out—I do not know if you are aware—the new Bill to amend the Commonwealth Act actually has brought in a small reform at least in respect of automated decision-making, which is that the APP entities will need to set out in their privacy policies certain information about the automated decision-making that they use. It probably does not go far enough, but it will be a very useful step if that finally ever gets enacted.

The CHAIR: Interesting. Thanks, Anthony. Thank you, Moira. John, I might go to you next.

John MULLAHY: Thanks, Chair. And thanks, Moira, for attending today. You just touched on artificial intelligence there, so I am just interested. In what ways could the use of AI in workplace surveillance impinge on workers' human rights?

Moira PATERSON: It would infringe particularly in terms of their right to equal treatment—to the extent that it discriminates against people based on protected traits. Certainly there has been evidence in the United States that for some ethnic groups or perhaps women or so forth it may produce different outcomes, so there is that one. It certainly implicates the human right to privacy. The whole process is dependent on gathering a lot of information about individuals. It is based on correlation, so you might feed into it data that does not fall under a definition of, say, sensitive data, but it can draw inferences from what is fed into it about people's medical conditions, their psychological conditions—all sorts of stuff that might itself be protected otherwise—and so that has massive privacy implications because it allows insights that, if they are correct, are incredibly accurate. They may be wrong, but to the extent they are correct they are capable of shedding light on a great deal about an individual: their motivations, their interactions with others and so forth. That implicates the right to privacy and also autonomy more broadly that underlies human rights in the sense that the more information that is held about you, the more you can be manipulated. We have seen that in political advertising and so forth. It is in a number of contexts—in the consumer context, with marketing and so forth—that the more you know about someone, the more you are capable of manipulating as well. I think those are the key rights that it bears upon.

John MULLAHY: Thanks, Moira. Cheers.

The CHAIR: Thank you. I might be able to squeeze one more question in, I think, Moira. Today we had a witness talk about neurotechnology—using brain patterns and technology that maybe, if you were fatigued or something, would either stimulate or talk to you or you would get a message or something to tell you you were

experiencing fatigue and things like that. I suppose I want to talk about the privacy of our biometric data and that sensitive information. Have you got thoughts on how we do that and protect those fundamental rights and our biometric data?

Moira PATERSON: One important thing is that in the current Privacy and Data Protection Act in Victoria, the category of sensitive data does not cover biometric data. I think that is an important amendment that needs to be made, otherwise I would say that is only going to be relevant to the public sector. I think the problem is that the private sector is only really dealt with under the Commonwealth Act, which is limited in that respect.

But I do think you are absolutely right. From the evidence you have received, we are really moving very fast down that direction of being able to infer very, very personal information that actually shows our feelings and our emotions, and that is certainly being used by marketers. They can tell from someone's telephone and the way they are using it whether they are a teenage girl who is feeling depressed and then they can bombard them with advertisements about make-up or things that they might be particularly responsive to when they are feeling insecure, say. You can see that already happening in the commercial sector, and I think it makes people very vulnerable right across the board, including in their employment relationship. To date, employers have only been able to glean information directly about your performance and how you behave at work and how you interact with people but not that much deeper information. This is not confined to the workplace context, but this is a context where there is a very grave power imbalance already and now you are producing that.

I mean, to the extent you have a sui generis employee surveillance law, you could bring restrictions in relation to that. Given the constitutional situation, I think the way that Victoria would need to regulate this is presumably through a surveillance law, because surveillance laws seem to be accepted as being within the state area and charter protection is Commonwealth, except as far as the state and territory public sectors are concerned. So it is difficult to go down the data protection route into the private sector without running into potential difficulties, but to the extent you have a surveillance law, which is I think perhaps the most practical solution given the constitutional arrangement, then there is nothing to stop you putting appropriate restrictions into that. Again, if you had a test of the necessity and proportionality, that should presumably exclude a lot of that because it is not really clear why an employer would need to know that. I mean, there are health and safety reasons why they might want to know if you are driving safely or certain situations, but then it would need to be proportional and necessary. I think that the value of something like a proportionality or necessity test is that it would of itself exclude that, but you could make it more explicit.

The CHAIR: Yes, and I was going to go to that—what is the necessity of that data that they are collecting or surveilling you for? But yes, thank you. Thank you so much. I am just mindful of time. I really appreciate you presenting and taking our questions today. It has been really insightful to get a different perspective, so thank you very much for your time.

Moira PATERSON: It was a pleasure. Thank you.

The CHAIR: Thank you.

Committee adjourned.