T R A N S C R I P T

LEGISLATIVE ASSEMBLY ECONOMY AND INFRASTRUCTURE COMMITTEE

Inquiry into workplace surveillance

East Melbourne – Monday 23 September 2024

(via videoconference)

MEMBERS

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

WITNESS

Professor Peter Leonard, Principal, Data Synergies and Professor of Practice, UNSW Business School

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

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

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

Thank you so much, Professor Peter Leonard, for joining us today. I will just quickly introduce the Committee to you. I am the Chair, Alison Marchant, Member for Bellarine. We have Wayne Farnham, Member for Narracan; Kim O'Keeffe, Deputy Chair and Member for Shepparton; and Anthony Cianflone, Member for Pascoe Vale.

Thank you so much for your work. Your submission was very interesting to read, and I really appreciated the submission. I might allow you maybe 5 minutes or so to make some opening statements or remarks and then we will jump straight into some questions.

Peter LEONARD: Thank you, Chair, and it is a pleasure to be invited before the Committee. Perhaps I should start with a little bit of background. I am still a lawyer, but I was a big-law partner for many years, a co-founder of the law firm called Gilbert + Tobin, and I led their data and technology and practice for 28 years. When I retired out of big-law practice I focused on the same kinds of businesses that I had been advising during my legal career, but with a broader focus around data and AI governance. That shift in focus really reflected an increasing dissatisfaction that I had—that people would ask me questions about whether something was legal, rather than the question of whether something was responsible and trustworthy. I wanted to shift the dial of the conversations with organisations that I was involved with, in order to give organisations a better understanding of what trustworthy data practices look like.

I had for many years worked with organisations that were using advanced data analytics and specific-purpose AI. Then, as the uses of AI and connected devices and so-called smart services became more pervasive, it became clear to me that the old ways of thinking about privacy and the use of devices to monitor the activities of individuals did not work anymore, in particular because of increasingly common surveillance of individuals in circumstances where they simply would not anticipate that their activities were being surveilled. Secondly, the surveillance and tracking devices were becoming so cheap and ubiquitous and easy to deploy, that organisations were deploying them much more than they were a decade ago.

That really got an impetus with COVID and working from home. Many employers rightly implemented surveillance technologies to deal with, amongst other things, the issue of whether you know somebody accessing employer systems from a remote location is in fact who you think they are and authorised to access those applications, or whether it might be a hacker or other unauthorised persons impersonating a proper user. So with COVID and working from home there was a big uptick in implementation of remote surveillance of employees. I think much of it was well-meaning and may well have been justified in terms of the underlying purpose. But it is probably fair to say that many employers did not properly understand the types of controls and safeguards they should be implementing as to how and when those technologies were used, limiting access to relevant surveillance information within the organisation, and were not taking proactive steps to inform employees that they were being surveilled in this way.

There was an issue as to breakdown of transparency, an issue as to breakdown in explainability and explanation. There was an issue in any event in applying existing frameworks of notice and consent to a workplace environment where, to be frank, I think consent just does not work as a concept with employees, particularly in a tight employment environment where employees are not going to be inclined to exercise their right to resign over an issue such as surveillance. So notice and consent does not work in environments where people are not able to readily exercise an ability to walk. In any event, the law did not really focus the attention of employers on concepts like necessity, reasonableness, proportionality and so on.

We are seeing in the proposed reforms of privacy law at the federal level introductions of new concepts like an overarching fair and reasonable test in relation to collection and uses of data as regulated by the federal Privacy

Act. The surveillance devices legislation in the various states is still based on outmoded concepts of notice and consent. There is not the explicit inclusion of concepts like necessity and proportionality, as well as transparency and explanation to affected individuals, so we have a situation where at the federal level we are moving towards new environments where we apply concepts like fairness and reasonableness, and we have not yet looked at applying similar concepts in relation to legislation around surveillance devices and tracking devices. Then in some states such as Victoria your statute is even further behind in the sense that it has not yet properly addressed data surveillance, which is one of the most common forms of surveillance nowadays due to the ease of implementation of it within organisations—keystroke monitoring and so on—and the regulation of tracking devices remains still in the notice and consent world, rather than moving to new concepts of fairness and reasonableness.

So my submission was an attempt to as it were simplify the complexity around this piecemeal and complex legislation and say, well let us go back to the basics of the principles that should apply in this area and then think about how those principles might be applied to legislation like this, rather than tweaking at the edge of concepts of notice and consent, which in my view are important but outmoded and insufficient.

The CHAIR: Thank you so much for that. We certainly have heard that in a previous hearing, about just getting that balance right. I might just jump to questions if we can and if that is okay with you, Professor. I might go to Deputy Chair Kim first.

Kim O'KEEFFE: Thank you. Thank you so much for your submission. I was actually travelling last night and I had another really good read of it, so I think you have almost answered most of our questions. You touched on the illusion of notice and consent with surveillance. Why is notice and consent problematic in terms of workplace surveillance, and how can laws be drafted to overcome this?

Peter LEONARD: I have a fundamental problem with the construction of many modern data privacy and surveillance laws in that they start from the concept that it is for the person who is being surveilled or whose information is being collected to have an active engagement with a notice and then, based upon that notice, make a decision as to the action that they take. I think that is fundamentally the wrong starting point. I think the starting point should be that organisations should be accountable as to how, when and why they collect information about individuals. We need to move away from a world where we place the burden on individuals to engage with notices about how information about them is collected, because we all know that we do not have enough time to read all those notices. We do not have necessarily the technical understanding to engage with them. It just is simply impractical and unrealistic to expect individuals to be making decisions about how information about them is being collected and used. So that is sort of the starting point, which applies economy-wide to all uses of data about citizens.

Then you move to the workplace, an environment where, by definition, there is an inequality of bargaining power between an employer and employees. That inequality becomes even starker as we move into an environment of cost-of-living pressures and high costs of mortgages and rents, where individuals are disinclined and disincentivised to, as it were, vote with their feet, if they do not like what employers tell them about how information about them is being collected and used. I think the starting point is we need to recognise these power imbalances and inequalities. So, let us shift the burden back onto the employer to make a reasoned justification for how and why they are collecting this information.

Then we have to get the balance right, because there are many circumstances I think in which employee surveillance is reasonable, necessary and proportionate. A classic example is where, as I said before, employees are working from home and the security issues around working from home are significant. It may be that in some cases of discipline in the workplace it is appropriate to be using technologies such as keystroke monitoring to actually work out whether people are working when they say that they are. I think it is reasonable to say that when you move away from the workplace, where there is visual surveillance of how and when employees are working, then there may be circumstances in which electronic surveillance of how and when an employee is working and whether they are working safely from home is a reasonable substitute for the physical workplace. But that will only be the case if you have proactive thinking and care around what the controls and safeguards are to ensure that this does not go too far and become yet another tool by which employers can unreasonably snoop upon all activities of their employees, including in circumstances where it is entirely unreasonable for them to do so.

The CHAIR: Perfect. Thank you so much. Wayne.

Wayne FARNHAM: Thank you, Chair, and thank you, Peter, for joining this today. I want to talk about surveillance used for the basis of dismissal. We have heard from unions. They tend to argue that they should not be using surveillance for disciplinary action or dismissal, based on what they see. I would like to get your thoughts and views on this. I mean, it is always a fine balancing act. You can get surveillance and someone might steal something and be sacked for that, but you do not want to see people disciplined for maybe having a 3-minute chat. So I want to get your views on that and where the balance on that could land.

Peter LEONARD: Look, it is a very good question. The fundamental issue is that the law does not prompt employers to properly consider the kinds of controls that they might put in place within their organisation to ensure that surveillance information is only made available in limited circumstances for limited purposes. That is something which is now well recognised in the privacy world, because there is a distinction drawn in privacy regulation nowadays between what is called 'effective anonymisation of information' and uses of personal information. That distinction really looks at what technical, operational and legal controls an organisation puts in place to ensure that information is only accessed and used in an appropriate circumstance.

To lead back to your question directly, Wayne, I think the fundamental issue today is that HR departments in many organisations have unlimited access to, amongst other things, data surveillance logs in respect of employees and may or may not make decisions as to the disciplining of those employees based upon that information, including in circumstances where the information may be simply unreliable but a person in an HR department does not necessarily have the skills to evaluate the reliability of that information. I think that a key aspect of reform should be not creating a blanket prohibition on the use of all surveillance information for any form of workplace supervision or any form of dismissal, but rather requiring that controls are put in place within an organisation so that if and when a decision might be made that affects an employee, there is then appropriate notice to the employee, there is a reasonable right to be heard, and then the decision that is made as a result of that surveillance is appropriate and proportionate to their action or inaction.

So I think a lot of it is about the technical and operational controls within an organisation. And how do you get there? Well, you start with the concept of employers being required to be fair and reasonable in their collection of information, in the sharing of information within an organisation and the use of that information. I do quite a bit of work in the privacy space and in relation to data security, and in both privacy and data security I say there are four common problems in relation to the practices of organisations. There is overcollection of information; there is overexposure of information within an organisation—that is, they do not put enough controls in place as to who can see what information and in what circumstances; the third problem is overuse, which partly flows from overexposure; and the other is over-retention—too many organisations retain information far longer than they need to retain it for the purpose for which it was collected.

So if you address all of those 'four overs', a lot of the problems in data privacy and data security would be ameliorated or reduced. I mean, we do not eliminate the problems, but they are four overs that have to be addressed. And then when you get to the surveillance world, you have got the additional problem that it is so cheap and easy to collect this information in so many ways nowadays, including through tracking devices on vehicles and use of work-supplied internet-connected devices and so on.

Wayne FARNHAM: Thank you.

The CHAIR: Thank you. Great question, Wayne. Anthony, I will go to you.

Anthony CIANFLONE: Thanks, Chair. Thanks again, Professor, for appearing. You have given a very, very detailed and comprehensive submission. Look, I just want to pick up off Wayne's point there but take us to artificial intelligence and the role of artificial intelligence in this whole debate and discussion. In doing so I just want to go back to something you said at the very beginning of your opening remarks. To paraphrase what you were saying, a lot of the conversations you had in past times with employers were around whether or not data surveillance or workplace surveillance is legal or okay or ethical. That conversation, starting from that perspective, I thought was quite interesting and profound—how that informs the illusion of notice and consent, essentially that notion of illusion.

So I guess in going to AI, before we do, I am just keen to point out that those conversations, whether with an employer or the lawyer and the employees, around workplace surveillance are still largely done with humans,

with human beings at the end of each of those conversations, but once we add in AI—artificial intelligence and algorithms—I mean, what is your view around how regulation can keep up with workplace surveillance in that space? And at a Victorian state level what can we do to anticipate a lot of those issues down the track where, if we have an illusion now of notice and consent, it is very much potentially going to be a mirage, well and truly, if we do not get in front of it now, I would hope through this inquiry. So what are your thoughts on AI in this space?

Peter LEONARD: Yes—again an interesting question. I start from the position that most of the applications of AI today are to assist or inform humans in making decisions that have certain consequences upon humans or the environment. So the first point of regulation is to recognise that AI generally is a tool or an aid to a human making a decision and then to ensure that the humans making the decisions properly evaluate whether that tool or aid is appropriate for the reliance that the human places upon it. And we have got, as it were, a window in time where we can educate humans as to appropriate evaluation of AI and how and when it should be used. And there are some things that we should be doing, such as tweaking rules around evidence so that humans are required to think hard about whether they use AI rather than use it as a crutch. A really good example is I think that there should be a reverse onus of proof such that when an individual uses AI as an assistant to make a decision then the onus is on that human to demonstrate that the AI was reliable for the reliance that they placed upon it, rather than the onus effectively being on a plaintiff to establish that the AI was unreliable. So there are things like that that you can do just by switching the onus of proof that really create incentives for people as they implement AI to think really carefully about how and when they should be implementing it.

The other thing to say about AI is that it can be a positive, as well as a negative. A good example is that modern surveillance cameras are being shipped today with AI capability built into the camera in the box. So if you go down to Officeworks today and buy an i-PRO Panasonic camera to put into your home, it will be capable of running at least one and in many cases four AI models at the edge. And why do I say that is a positive? Well, it is a positive because if you can run an AI model at the edge and you put the right controls in place as to who can access that information, you can control whether that information flows back into other systems and potentially is vulnerable to overexposure, overuse or over-retention at the back end. The other thing that AI can do is generate synthetic data, which strips out personal identifiers of individuals at scale and speed.

AI has got some real challenges to ensure that organisations are careful about using its powers, but it also has some superpowers, as it were, that can be used to control flows of data that otherwise create risks for employees. It is a two-edged sword. I am very nervous that organisations are implementing AI much faster and without adequate consideration of how to do it carefully and well, but I am also quite an optimist for how AI that is well deployed can reduce the costs of businesses doing business and actually improve privacy of individuals, if and when well done, which it usually is not today.

The CHAIR: Yes. Thanks, Anthony. That was a great question. The nervousness, I think, is being felt by all the Committee members.

Thank you, Professor. I am really sorry; we are out of time at the moment. We could have asked you a whole lot more questions. We appreciate the work that you are doing, in the submission, and for you having us ask questions today as well. We really appreciated that. Thank you for your time.

Witness withdrew.