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

WITNESSES

Associate Professor Normann Witzleb, Faculty of Law, Monash University, and Faculty of Law, Chinese University of Hong Kong; and

Murray Brown, Barrister and Solicitor.

The CHAIR: Welcome to the public 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 transcript to check, and 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 to minimise that interference.

Thank you so much, Normann and Murray, for joining us today and having a few questions from the Committee members in this inquiry. We have had a really interesting day today talking about a whole spectrum of issues that have come about, and I think this one is going to be another interesting conversation; I am really looking forward to it. What I might do is allow you to have a few minutes. If you would like to make any opening statements or remarks or a little bit of background, we are happy to do that, and then we will jump straight into some questions.

Normann WITZLEB: Thank you very much for the opportunity to speak to you today. I am a legal academic. I used to work at Monash University, and now I am at the Chinese University of Hong Kong. My research areas are indeed in data protection and privacy, not workplace surveillance specifically, but I think the background for you inviting us to speak to you is an article that Murray and I published a few years ago in the *Australian Journal of Labour Law*. I think a good place to start basically our conversation today would be that I just summarise some of the conclusions that we made in this article, and then perhaps we can take that as a springboard for any further questions.

Our conclusion was that workplace surveillance in Australia is currently governed by incoherent patchwork of laws which on the whole provide little protection for employee privacy. As matters stand, the growth of surveillance capacity, coupled with limited legal protections for employee privacy, particularly for private sector employees outside of New South Wales and the ACT, creates an environment in which surveillance of employees both at work and in their private life could grow largely unchecked. The sociotechnological developments over the last decades have made employee surveillance easier, cheaper and more pervasive. Employers increasingly, for example, scrutinise the personal social media engagement of their employees or use employer-provided devices, including wearables, to monitor them. The rise of AI-supported people analytics also promises employers improved economic returns from data-driven human resources management. The move towards flexible and work-from-home labour arrangements has further accelerated the trend to increase surveillance and led to a greater blurring of the division between work and private life.

Our article proposed nationally uniform legislation as the preferable way forward, not least because it offers an efficient approach to addressing the uncertainty that employers operating in multiple jurisdictions currently face. As to the regulatory approach this legislation should take, the Victorian Law Reform Commission's model still has much to commend it today. It is from 2005, but it combines a general prohibition against employers unreasonably breaching their employees' privacy with regulation for different types of surveillance that increases in stringency depending on the intrusiveness of the practice in question. Of course we are speaking now to the Victorian Parliament. We know that nationally uniform legislation is perhaps the most desirable way forward, but perhaps, as happened in the past, some state or territory legislatures need to move forward and perhaps get others on board. We will have to see to that.

The CHAIR: Yes, perfect. Thank you so much. Murray, was there anything that you would like to add first?

Murray BROWN: Not really; I just thought I would introduce myself. My name is Murray Brown. I am a barrister and solicitor. I was formerly a lecturer in law at Murdoch University prior to retiring in 2020, and I suppose for the last decade most of my research focus was on workplace privacy and in particular workplace surveillance.

The CHAIR: Perfect. I think we will have great questions for you both then. Kim, I might head to you first.

Kim O'KEEFFE: Thank you so much. Thank you for your submission. It is always great to go through the variety that we have had and the different things that come through, and some similarities. Social media is probably a bit of an interest to me. I think it is really interesting to see what the future looks like and particularly when it comes to work surveillance and being able to trawl and see what your employees are doing. There has been some recent media interest in whether employers should be allowed to trawl employees' social media posts. In which situations is it valid for employers to access employee social media posts, and when does it breach workers' privacy?

Murray BROWN: Okay, well, I will have a go at that. In my comments I am drawing on an article that Chris Dent and I had published in *Monash University Law Review* in 2017 entitled 'Privacy concerns over employer access to employee social media'. I think this does raise some really interesting questions, because on the one hand I have seen it argued that the ability to share information about ourselves, to participate in the community, reflects an integral aspect of an individual's right to self-development and indeed what it means to be human. And I have also seen it argued that there is a risk that if we allow employers to freely monitor what their employees are posting in their personal time on social media, that those employees—those individuals—are going to feel obliged to regulate their disclosure of information about themselves online to protect their core role as an employee, possibly at the cost of their ability to develop other aspects of their personal identity, so that in some sense an individual—an employee—may feel they are never off duty.

I have also seen it suggested that for members of the younger generation, they view an employer accessing even their public online profile like people of my generation might view an employer showing up at a private party uninvited. There is certainly no doubt that social media does potentially give employers unprecedented access to what once had been considered an employee's private life. But on the other hand of course there is the potential for damage to be done to employers by their employees' social media postings. I have seen another author comment that social media provides new and expanded opportunities for various forms of employee behaviour, including mocking the management practices, individual managers and customers and pursuing interests that may conflict with professional obligations, such as theft of intellectual property and bullying and harassment of colleagues. So clearly there is a balance that needs to be struck there. How shall I address you? Is your first name okay? Kim is okay?

The CHAIR: That is fine. Use our first names.

Kim O'KEEFFE: Kim, thank you.

Murray BROWN: That is good. Yes, I think there is clearly a balance that needs to be struck here. What I would like to see utilised here is the concept of proportionality. Is that a concept that you are familiar with?

Kim O'KEEFFE: Not fully.

Murray BROWN: All right. Something I did explain a bit earlier –

The CHAIR: Certainly, Murray, proportion has been said many times in this inquiry—'What is a proportionate surveillance?'—but I do not think it has been very clear to us. What does that look like?

Murray BROWN: Okay. The definition of 'proportionality' I have got is—and this is a concept that is commonly used in the human rights context, although curiously not so much in the context of privacy law in Australia—firstly, that any interference with the right—the human right, in this case the right of privacy—should be the minimum necessary for achieving a legitimate aim and justified in the sense that the societal benefit of the interference outweighs any adverse privacy effect. It is a matter of balancing the competing societal interests.

With that in mind I think I would make a few observations on this question of employer monitoring of their employees' personal social media. I think routine surveillance of even public social media posts of all employees should rarely, if ever, be necessary. It might be more justifiable to routinely monitor high-risk employees, but generally I think I would like to see employers' ability to monitor their employees' social media limited to workplace investigations where the employer already has some specific information suggesting employee misconduct. I think that certainly should be true where so-called private—password-protected—pages are concerned. I do not know how much of a problem it actually has been in Australia, but a number of states in the United States have passed legislation prohibiting employers demanding social media passwords off

their employees in the absence of a workplace investigation based on specific information suggesting employee misconduct.

The CHAIR: Interesting. Thank you for that, Murray. I might head to another question so we can get to a lot of different topics. Anthony, I will go to you next.

Anthony CIANFLONE: Hi. Thanks again for appearing, Normann and Murray. My question is around the notion of a workplace privacy regulator. We have heard quite a bit of evidence about and even some calls and suggestions for the establishment of an independent workplace privacy and data workplace surveillance-type regulator. In your view or in your opinion what are the pros and cons in establishing such a regulator? Could an existing agency potentially take on this role, whether that is WorkSafe or WorkCover potentially? Or should a new entity altogether potentially be looked at to be set up to oversee this whole world of workplace relations and workplace data collection and surveillance?

Murray BROWN: Did you want me to answer that or give Normann an opportunity?

Normann WITZLEB: I could have a go at this one. Basically, if you are talking about workplace privacy and workplace surveillance, it is still part of privacy and data protection more broadly, even though it occurs in the workplace. An important point is that a regulator has sufficient powers and has sufficient resources to investigate matters if needed, and it is important also that they have sufficient status to make proposals and make guidelines and so on. I am not a regulator of course, but from an academic perspective I would say the preference would be to give that task to an existing regulator. I think probably OVIC might be in a better position to do that than a separate regulator. The important point about data protection and privacy legislation is that much of it is principles based, so it is not always clear whether a particular practice is permissible or prohibited; it depends on context very often. If you have a number of regulators with overlapping responsibilities, there is of course a chance of confusion and of disparate standards being applied.

When it comes to workplace privacy, employers generally have, collect and use a lot of different data—customer data, employee data and the like—and if you have rules that as far as possible are common across the different areas, if you have regulators that as far as possible are common across the different types of information, you generally make it easier for employers to understand their obligations and also to comply with their obligations. I would probably suggest that you should draw on the expertise of OVIC as a privacy regulator. Particularly in the Victorian context they are regarded as even handed, as proactive and many other things. Draw on that expertise to basically have a more common understanding and a more common standard for various types of workplace-related as well as other information that employers are likely to collect and use in their daily practise.

Anthony CIANFLONE: Thank you.

Murray BROWN: Can I add something there?

The CHAIR: Yes, sure, Murray.

Murray BROWN: I would agree with Normann. I note that the Victorian Law Reform Commission did in its report advocate for a one-stop shop independent workplace privacy regulator, but I tend to agree with the points Normann has made; I do not see any need for a specific workplace privacy regulator that is separate to the existing privacy regulator. One thing I would add, though, is that I do think it is important that there is a specific regulator responsible for the administration of any workplace surveillance legislation. It does not necessarily need to be a separate workplace surveillance or workplace privacy regulator, but somebody does need to have responsibility for its administration. The reason that I make that as a point is because as we said in our article, one of the criticisms that has been made of the New South Wales legislation is that it does not have, or did not have, at least, at the time we wrote our article, a specific regulator responsible for its administration. That had resulted in the New South Wales privacy commissioner calling for a regulator to be given power under the New South Wales Act to inspect workplaces, investigate and resolve complaints and prosecute offences. It is possibly for that reason—that there had not been a specific regulator given responsibility for its administration—that at the time we wrote the article, even though there had been, according to the New South Wales privacy commissioner, a number of complaints in relation to workplace surveillance, there had not actually been a successful prosecution under the New South Wales legislation.

The CHAIR: Thank you for that, Murray. John, I am going to squeeze one more in. I am going to go to you.

John MULLAHY: We have had submission after submission after submission discussing the European Union's data protection laws as best practice. To what extent should Victoria adopt aspects of these laws but specifically around the workplace surveillance data?

Normann WITZLEB: Let me start with that one because I have worked on the European data protection laws and contributed to commentary on the general data protection regulation in Germany. The important point to bear in mind is that the general data protection regulation, the GDPR, is a data protection statute, so it deals not specifically with surveillance; it deals with data processing more broadly: anything from the point of collection of data all the way through the different types of data handling up to access, correction of data and then also deletion of data. There is an overlap with surveillance because surveillance is a form of collecting data. But you cannot replace one with the other, so there is still a need for specific surveillance legislation because it deals with particular types of surveillance, in what circumstances it is permissible and the like.

I would hesitate to recommend wholesale adoption of a form of the GDPR in Victoria. The problem is that we already have data protection laws at federal level and of course in Victoria, and it is important that you basically respect the specific rights context in each of those jurisdictions and that you do not add another layer of complexity to it. The GDPR is embedded in the specific European human rights context. In Europe there are actually two rights in the European charter that deal with privacy and data protection, so that is different to what we have in the Victorian context, for example, where there is only just the one dealing with privacy. It has also developed a very sophisticated jurisprudence around them. Murray earlier made the point about proportionality. Very often practices under the GDPR are not as such allowed or prohibited, but it is about balancing of competing considerations. Of course it is privacy or the right to data protection that is on the one hand of the balance, and then the competing considerations—you have heard evidence about many of the employer-related considerations, such as protection of assets, protection against liability and other workplace matters—need to be balanced. The GDPR allows for that balancing in the way that it structures the obligations. If you did the same and tried to emulate that in Victoria, it would be important to align whatever you introduce with the framework that exists already in Australia.

My earlier point was that when it comes to regulators, it is important to not have too much overlap and possibly differences of standards between regulators, and the same applies actually at the point of the substantive laws. It is more important that you have laws within Australia that are adapted to what they need to achieve and that are aligned with one another, so I would probably not advocate wholesale adoption of the GDPR in Victoria or a version of it. But what happened, for example, in the discussion at the federal level when the reform of the Privacy Act was being discussed is that the GDPR was used as a reference point, and that is probably the preferred way—you look at what regulations are there in the GDPR and to what extent they are transferable into the specific context that is in place in Australia or now here at the state level in Victoria.

The CHAIR: Thank you for that. I am really mindful of time. I think we have a whole lot of other questions we could have asked you today, and I am really sorry we have run out of time to do that. But if there is something you think that the Committee needs to understand further, we would more than welcome and accept any more evidence if you would like to send us any of your research or further links that we might be able to reference. Thank you so much again, though, for your time.

Witnesses withdrew.