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

Dr Jean Linis-Dinco.

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 the 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 just remind members to mute their microphones when not speaking to minimise any interference.

Thank you, Dr Jean, for joining us today. What we might do is give you a few minutes just to talk a little about your submission and maybe a little bit of background, and then we will jump into some questions for you.

Jean LINIS-DINCO: First, I would like to thank the Committee for the opportunity to speak here today. My name is Jean Linis-Dinco, and I am a worker. Much of the conversation around workplace surveillance in and outside of Australia has taken into account voices of the private sector, business owners, academia and even trade unions, but today, I stand before you online not as part of any organisation but as a working-class woman striving in this economy to make ends meet. My intervention comes from a cybersecurity and human rights perspective. While I know that I may not command the same authority as prominent voices from the sectors I mentioned previously, I believe that my presence here underscores the democratic principle that every voice matters.

Regarding my submission, the concept of surveillance in the workplace is nothing new. History can tell us so many examples of how surveillance was used to control a workforce, but what is new is how cybersecurity threats have been portrayed as an existential problem, which needs extraordinary measures. The way this works is that it has facilitated this normalisation of practices that would not otherwise be viewed as draconian under typical circumstances. In these scenarios, we see how employees are treated as potential threats. They are securitised and they are scrutinised, which alters the very foundation of the employee–employer relationship. What workers face here is not a safeguard but a presumption of guilt—an assumption that undermines labour rights and dignity in the workplace.

The CHAIR: Thank you so much for that. It is a different perspective that we hope to have a conversation with you about today. Wayne, I might go to you first, thanks.

Wayne FARNHAM: Thank you, Chair. Mabuhay, Dr Linis-Dinco. How are you? That is Filipino for 'Hello, everyone'. It has been interesting today with the discussions that have been going on. One gentleman, Dr McCay, before you came on, talked about the neurosurveillance that is now being used with some employees—monitoring brains so that if you are getting tired of work, you get notified and everything else, which, to be honest, scares the hell out of me. This leads to artificial intelligence and machine learning. In what ways could AI and machine learning, using workplace surveillance data, harm workers?

Jean LINIS-DINCO: So, machine learning is primarily the technology behind the infamous user and entity behaviour analytics, or UEBA. These systems work by creating detailed profiles of each worker's behaviour, noting how they use applications, access data and even their login patterns. So, by continuously profiling and assessing behaviour against a normal baseline that they set, these systems place every employee basically under a microscope, and this continuous scrutiny can foster an environment of suspicion and fear. Employees might feel that every action, no matter how innocent, can be misinterpreted as malicious by an algorithm. This sort of surveillance breeds a culture of paranoia where employees feel that they must constantly prove that they are not threats, and these AI-driven systems we know that they are not infallible. They rely on patterns and data which can lead to incorrect assumptions. An algorithm might flag a well-intentioned action as, let us say, suspicious simply because it deviates from the majority or deviates from what is expected or what is normal and not because it poses any real threat. And the consequences of such false positives are not trivial. They can affect a worker's performance reviews, professional relationships and even their career trajectory. And on top of this is the question of opacity of this system, which also compounds the whole issue, because workers are often unaware of the full extent of the monitoring or how the data about their behaviour is interpreted and stored.

So I go back to my previous example, or metaphor, of how a cybersecurity threat is suddenly being viewed as an existential threat to a certain referent object, which is corporate integrity, let us say. And that kind of portrayal elevates the issue to a matter of extreme security to justify these extraordinary measures. The way these bosswares work is not restricted to professional tasks but often extend to personal communications and other behaviours that occur during work hours and beyond. We have systems that are designed to create profiles based on behaviours, systems such as Microsoft Purview, which has the insider risk management that operates by calculating scores for various incidents, essentially quantifying employee action into risk assessment. So right now every worker is a quantified worker. By having a system that assigns scores to workers through certain risk policies, we take away the dignity of the worker and turn them into mere statistics.

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

Anthony CIANFLONE: Thank you, Doctor, for your submission and for your evidence. Because you have previously done quite substantial work through your thesis on the use of machine learning techniques in the Rohingya crisis in Myanmar, can you just talk to us a little bit about what your insights and learnings were through that research and what actually happened there, as briefly as possible, in terms of that applying to a Victorian context and how that is potentially relevant and what we should be mindful of as part of any recommendations?

Jean LINIS-DINCO: Yes. You have put me on the spot asking about it.

Anthony CIANFLONE: I know it is a big question, but it is important. I think it is important to put on the record.

Jean LINIS-DINCO: Yes. So, my research in Myanmar focused on the Rohingya crisis and how the government—not just the government of Myanmar but spectator countries like India and Bangladesh, for instance—have coopted the narrative of certain portrayal of the Rohingya people by the Burmese government. In that space, I have learned quite a lot of things on how propaganda works and how divisive culture can lead to a mass genocide and expulsion of people in their home and in their workplace. I do not think that there is a similarity with workplace surveillance and my thesis, unfortunately, but one thing I can say is that the use of machine learning in this regard for a human rights case or a human rights related issue is a very sensitive issue. It must take into account all the necessary human rights that we have at the moment—you know, the right to privacy and the right to redress, which is a very good example in this space.

I would probably say that the right to redress here is the most fundamental principle in safeguarding employee rights, particularly in the context of workplace surveillance and data protection. I believe the person who spoke before me mentioned something similar. I believe that this right to redress ensures that employees have accessible, effective avenues to address grievances and seek remedies if their personal information, for instance, is mishandled or their privacy is breached by their employer. When employees feel that their rights have been violated, be it through unauthorised access, improper data collection or misuse of personal information, they should have the means to challenge these actions and receive compensation or other forms of redress. This process not only upholds individual rights but also reinforces a culture of accountability. Not to repeat most things Dr Fiona said, but a culture of accountability is crucial to trust in the workplace.

The CHAIR: Thank you, Anthony. Thank you for that. I am mindful of time, but John, I think we have time for a question from you.

John MULLAHY: Thanks, Dr Linis-Dinco, for being here. What I would like to know is: what safeguards should Victoria set up to ensure workplace surveillance is targeted and proportionate?

Jean LINIS-DINCO: In my submission, I mentioned 'proportionate' and 'targeted', and I would like to also mention 'limited'. When I mentioned those words, I was really talking about creating an environment that respects individual privacy in autonomy. To cite a recent draft that UNESCO released a few weeks ago, they released a report on certain AI approaches globally. One that struck me the most is the difference between an ethics-based approach—a principle-based approach, which is the ethics-based approach—and a human rights-based approach, and I believe that we should be taking a human rights-based approach to address legitimate organisational needs. So, that means that there needs to be legislation that would ensure that surveillance is not just implemented because it is technologically possible—you know, it serves broad managerial interests because it is generally needed for a specific, justifiable reason. When I say surveillance must be necessary, it

means that measures should only be implemented if there is a clear, unavoidable need for them that serves a specific purpose like protecting sensitive information that if leaked could genuinely harm people. A law should definitely require that any proposed surveillance be the only viable option to achieve this security objective, thereby preventing the use of invasive tools when less intrusive alternatives would suffice.

Then there is 'proportionate, which implies that the extent of surveillance should not exceed what is needed to address the identified need. This means that surveillance's impact on privacy should be reasonable in relation to the benefit gained from it. So when we talk about surveillance being limited and targeted, we are focusing on ensuring that monitoring is confined to specific areas that are directly related to identified risk rather than being broad and unfocused. For instance, if there is a concern about data breaches from a particular, let us say, department that handles sensitive information, then the surveillance should be limited to that department's operations and not extend to other parts of the organisation where the risk does not apply.

John MULLAHY: Thank you.

The CHAIR: Thank you so much. I am mindful of time, and I think we could have asked a whole lot more questions, but I am sorry we will have to end it there. What I want to say, though, is if the conversation today has sparked any further information you would like to provide to the Committee, we can certainly accept further information from you, and we would welcome that as well. Thank you very much for your time today.

Jean LINIS-DINCO: Thank you very much.

Witness withdrew.