# 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**

Professor Peter Holland, Professor, Human Resource Management, School of Business, Law and Entrepreneurship, and Dr Jacqueline Meredith, Lecturer, Swinburne Law School, Swinburne University of Technology.

**The CHAIR**: I begin today by acknowledging the Wurundjeri Woi Wurrung people of the Kulin nations, the traditional custodians of the land on which we meet today. I pay my respects to elders past, present and future and extend all respect to all Aboriginal and Torres Strait Islander peoples here today.

I advise that the sessions today are being broadcast live on the Parliament's website. Rebroadcast of the hearing is only permitted in accordance with LA standing order 234.

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 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.

Before I invite you to make an opening statement I thought it would be best if we introduce the Committee to you today. Then we will go to you for about a 5-minute opening statement. We have got lots of questions to put to you, so I will keep that very short, the opening statement, then we will go into questions. Thank you.

**Kim O'KEEFFE**: Good morning. I am Kim O'Keeffe, the Member for Shepparton.

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

**John MULLAHY**: John Mullahy, the Member for Glen Waverley.

**Dylan WIGHT**: Dylan Wight, the Member for Tarneit.

**The CHAIR**: And I am Alison, the Chair and the Member for Bellarine as well. Over to you.

**Peter HOLLAND**: My name is Peter Holland. I am a Professor of Human Resource Management at Swinburne University. One of my key research areas is electronic monitoring and surveillance, particularly in the workplace. That is where my strength lies. I have done several research projects and I have published extensively in the area, hence my interest when I was asked about getting involved in this, because I think it is a really valuable opportunity to catch up with the law in terms of where the technology has gone.

**Jacqueline MEREDITH**: Thanks, Peter. I am Jacqueline Meredith, Lecturer at Swinburne Law School, Swinburne University of Technology. My area of expertise is more on the legal regulation of workplace surveillance. I have looked in quite some detail at the existing Victorian framework and what we might learn from other jurisdictions in the country.

**The CHAIR**: Perfect. Do you want to speak a little bit to your submission?

**Peter HOLLAND**: Yes, can do. I am very conscious—half an hour—you want to ask questions, and being academics we could talk forever.

**John MULLAHY**: We are politicians, so we are about the same.

**Peter HOLLAND**: And you are politicians, so this could be a bit of a tense stand-off here I know. I understand. But look, I think the key thing I particularly want to talk about—we have all been through the pandemic obviously—is that we have significantly changed how we work, and I do not think many people have really grasped the significance of it. Traditionally you would get up, like I did today, leave your house and come to a work environment and go home again. Now—and you are probably the same—you work at home; there are no natural boundaries anymore between working here and working at home. You can do all that on Zoom and Teams.

My concern—I started doing research when we went into lockdown—was the amount of surveillance that started to appear on computers. Gartner did a global study during the early pandemic that showed 80 per cent of private companies were putting what they call euphemistically 'tattleware'—monitoring and surveillance—on

people's work computers at home without telling the workers. In Australia it was 90 per cent, so we are even more distrustful in this country. It comes from two things: one of these is a thing called the flexible paradox—the more flexibility give to people to work anywhere they want, the more companies were getting more paranoid about, 'Well, if I can't see you, are you really working? And how much time are you spending at work and not at work on your computer?' The other one is productivity paranoia where they are paranoid that, 'If I can't see you, you can't really be as productive as if I'm standing over the top of you.'

It is that 19th and 20th century sort of model of management turned into an electronic unblinking eye, and we have accepted it, we all take it on board and we do not really think that it is significant. I have got two boys in their 20s; *Nineteen Eighty-Four* to me is a very dangerous novel, to them it is a show on the telly. I keep telling them how much the stuff they put on the internet is there forever, but it is a different generation. So I think it is important that we have got a chance here to maybe put some regulations in. And before I just throw to Jackie, the best example I have got: I have taught postgraduate at both Swinburne and when I was at Monash, and I ask students, postgrads who are HR managers, 'Do you monitor and surveil your workforce?' And they say yes, and I say why, and they say, 'Because we can'—because there is no legal regulation to stop them. And I think that is the boundary that I am concerned about. But I am not the expert.

**Jacqueline MEREDITH**: In terms of existing regulation in Victoria, as we outlined in our submission, it is limited in scope for workplace surveillance. For the most part workplace surveillance in Victoria is regulated by those more general surveillance provisions. We only really have one or two specific workplace surveillance sections in that general legislation. That is not a good approach. We would advocate for specific workplace surveillance legislation which is more in tune with the nuances of the employment relationship and the imbalance of power that frequently exists in that relationship, and I guess that is probably most obviously exemplified in the current legislation on the consent basis that exists. If a worker gives consent, and it can be implicit consent, that is going to be sufficient, and that is not really in tune with the nuances of the employment relationship. The fact is that workers will often feel like they have to give that consent, otherwise they will incur negative consequences such as dismissal.

**The CHAIR**: Yes, perfect. Thank you for that. I think that is a good start for us as well. I will go to our Deputy Chair.

**Kim O'KEEFFE**: Thank you. And you did touch on our first question, which was pretty much around the impact from COVID. How have the boundaries of privacy in the workplace changed since the pandemic? You have touched on that.

**Peter HOLLAND**: Yes. To expand on that, the other factor is that since we did that study in 2021, the level of surveillance has improved, if you want to use the word 'improved'. They can pick up background conversations now. A lot of these systems are on continually. The euphemism is the unblinking eye—it is just there watching and hearing. So if you are having a conversation in the background, it is picking up private information. Who is storing it? Who is taking it? How long is it being kept for? Is there potential for it to be hacked? I mean, there is so much they can pick up in the background, which also concerns me. If an employer has to tell you that it is conducting monitoring and surveillance and what it is doing with that information, then people may be more cautious, but also as well it makes the employer more responsible for just taking that information in. I think that is the thing I am more concerned with, because I could be on my computer and there are conversations going on in the background that are nothing to do with work but they are being picked up by work. So that would be my concern.

**Kim O'KEEFFE**: Yes, which pretty much leads into the next question: what impact could this have on workers and their families?

**Peter HOLLAND**: I did a national study in 2017 on monitoring and surveillance and we found a direct correlation between the more electronic monitoring and surveillance there was, the less trust the workforce has in their employer. Trust goes down and productivity also goes down. There is a paradox here where the more you surveil people, the less productivity will occur, and then people start doing things. For example, if I am being monitored to be writing all the time and Jacqueline has got a problem, if I go and help her, that takes me away from the productivity. We gave an example in our report about a journalist in New York who had done this and found that he was considered to have only been working 18 hours when he had done 48 because the surveillance is making you only comply with what is being surveilled. Again, I am trying to give employers the

economic argument, which is that the more you surveil people, the less productivity you will get. It is not a case of it being one side or the other. There is a really strong economic argument for this as well.

**Kim O'KEEFFE**: Thank you.

**Anthony CIANFLONE**: Thank you, and thanks for your submission as well. I have gone through it all, and it is very comprehensive. You gave the analogy at the start of *Nineteen Eighty-Four*, which I very much acknowledge and see the relevance of. But the other analogy you gave in your submission was around panopticons. Panopticons kind of represent the area of Coburg. We have two of Australia's last remaining—I believe—at Pentridge Prison, which are still on display. I think there is a lot of relevance in terms of that analogy of panopticons of the 19th century criminal justice system and how that applies to almost a modern-day panopticon in terms of workplace surveillance. So maybe if you could talk a little bit about that and also how the effectiveness of the current laws in Victoria can be strengthened to sort of negate—

**Peter HOLLAND**: Well, I can do the first bit. That leads on to what I was saying before about if you feel you are being surveilled. Often I will do this for the students as an example when, surprise, surprise, they have all got their computers up but they are not all necessarily looking at the work they should be—if I, say, start wandering around the back, people just become uneasy if they feel they are being monitored and surveilled. And then, as I said earlier, they will observe certain ways of working to make sure that they are covered because of the perception that they could be being watched. They might not be, but there is always a perception someone is watching them, so people will then start conforming and doing what is required to cover themselves as opposed to helping someone else, taking an extended break. Again, we had an example in there of people at Barclays Bank in the UK three or four years ago, the stress they were under if they left the workplace or they went to the toilet and then they would be logged out because the toilet break was too long. I mean, if you get to that level, you can see it stresses people, WorkCover, economic productivity all go down. But in terms of the legal aspects of it—

**Jacqueline MEREDITH**: I would say probably the biggest change we would need in the current regulation of workplace surveillance in Victoria is a proportionality-type aspect in the legislation. Yes, workers can consent to surveillance, but like we mentioned previously, that is not really a sufficient safeguard because workers will often feel like they have no choice but to consent. A strength of the approach in some other jurisdictions—New South Wales, the Australian Capital Territory—is that they do not have this consent-based framework; it is more of a notice and disclosure type framework, so the employer has to give notice that surveillance will be happening. The ACT is a little bit more advanced in terms of the specific details of that surveillance notice, but in both jurisdictions you have to tell the workers these are the specifics of the surveillance, this is the start date, this is the purpose et cetera. I would say the approach in those other jurisdictions is definitely something we could take some things from for Victoria, but it is certainly not perfect and it will not address all of the issues.

In particular, the approach in those other jurisdictions does not have this necessary proportionality-type aspect, so there does not have to be this legitimate purpose for surveillance. If the employer gives workers notice that it will happen and they comply with all the disclosure requirements, as long as those notice and disclosure requirements are complied with, the surveillance can happen. And there is no requirement that it is proportionate or that it achieves the legitimate aim through the least intrusive means possible. So I think to overcome a lot of these issues, that proportionality aspect is what is missing.

**The CHAIR**: John.

**John MULLAHY**: You mentioned about the tattle software being on people's computers, that sort of thing. People are working from home now—my concern is that you said it is picking up conversations in the background. My partner works from home, I will be doing work from home. How would we define the workplace to ensure people working remotely or from home are adequately protected? You mentioned implied or explicit consent by the employee—well, if they are picking up information of other people in the household, how are we protecting them and their privacy?

**Peter HOLLAND**: And people under-age as well—kids.

**John MULLAHY**: Correct.

**Peter HOLLAND**: That is a great question: what is the workplace today? And basically it is work from anywhere. We also work from home. But yes, it is not workplace—I think we mentioned that—it is workspace. I have a defined place in my home. A study we did, which was UK based, was talking about how companies adapted. We interviewed a series of people, and they said, 'Well, we were just told to go home, the COVID thing would be over in a few weeks'—from Melbourne we can appreciate that that is not quite how it happened—and they said, 'I was working from the kitchen table,' all sorts of things. It is probably more an issue where the employer has to be aware that, work from anywhere, there needs to be explicit things. It might be here, it might be at home, it might be at the university, but it is literally work from anywhere.

So if you have got your computer open, I think people need to be aware that the conversation is being picked up. Most of the tattleware was put on without people knowing, and they only found out that they were being photographed every 10 seconds or the speed of their keys was being monitored when they got an email saying, 'Where are you? What are you doing?' and they went, 'Where has this come from?' Those companies were not telling people. Again, it is like anything—there are implicit requirements at work of how you act and what you do, but I think with this sort of stuff there are no boundaries. The companies can just put it on. They are not breaking any laws. They are saying they are protecting their productivity, their people are not writing inappropriate emails and stuff like that. But it is really work from anywhere; it is workspace not workplace anymore. That is how I would define it. From the legal side—

**Jacqueline MEREDITH**: We do have some specific provisions in the current workplace surveillance legislation—sorry, just general surveillance legislation. There are not workplace specific provisions in the Victorian legislation, but there are general surveillance provisions which could be applied to the workplace. Section 7 in particular says the employer is not allowed to film private activities, and of course if you are working from home, you would probably have an assumption as a worker that a lot of things you are doing in your home are private activities. The problem is that that kind of exception is not going to be applicable if the worker once again gives explicit or implied consent, and often workers are going to give this consent. It might just be a sentence in their contract of employment. Often the employer will take a kind of catch-all type approach and have a very general and vague sentence in a contract of employment or workplace policy which says that the worker must consent to these types of devices. There will be no specific details of what their rights are or the scope of these devices. So as long as you have given that consent, the employer can film these private-type activities.

**John MULLAHY**: But there no jurisdiction here that has anything with regard to the consent of others that would be in the sphere of a device that is doing surveillance.

**Jacqueline MEREDITH**: No.

**John MULLAHY**: No. And even when we look at New South Wales or the ACT, nothing of that nature?

**Jacqueline MEREDITH**: No. The definition of what is private—what is a private activity—can be really quite ambiguous in the legislation. Does it capture just the location, or does it also capture the performance of work? It is very ambiguous about whether a private activity is something that you are doing even if you are at the workplace. For instance, if you are working from home, can you still be doing a private activity if your whole house is the workplace, or is anything you do in that location no longer a private activity because that is your workplace? The legislation really does not kind of go into the detail about that in New South Wales or the ACT.

**Peter HOLLAND**: I think part of this as well is that, especially in this state, we have come through the pandemic. I have been around a long time in academia. I was saying to students recently that in the last five years the workplace has changed more than the previous 25, because we do work from home. All those platforms were there, we all move fairly seamlessly, but I think there was always the productivity paranoia that employers did not want people to work at home because they could not see them and trust them. We have had various companies who are pressing their workforces to come back and other state governments who are encouraging their workforces to come back full time. People do not want that. But we have not allowed for the workspace to be anywhere and monitoring and surveillance to be everywhere as well. I just think we have accelerated. We have accepted where we are now: work from home, new normal. But that sort of managing your private life is a real, real issue and tension that we have not caught up with.

**John MULLAHY**: Thank you.

**Dylan WIGHT**: Thank you. I think this is probably going to be a common theme throughout this Inquiry and, Jacqueline, you have already touched on it on some laws that exist interstate, both in New South Wales, which was passed in 2005, and the ACT, in 2011. How effective are those laws in combating some of the behaviour that we have spoken about, particularly in an environment where things have changed significantly? Just following on really quickly from that as well, what can Victoria learn from it but also how does that legislation intersect with something that may be in an industrial instrument? With that sort of legislation and the protections within it, are we seeing in New South Wales and the ACT that that is stopping this sort of behaviour that you spoke about with a paragraph or a line in an employment contract that once you do your interview and accept employment, you just sign it half the time without reading it?

**Jacqueline MEREDITH**: Yes, thanks for the question. In terms of what Victoria could learn from these other jurisdictions, there are definitely positives in the approach taken in New South Wales and the ACT. There are the notice and disclosure requirements. Like I mentioned before, the ACT has a lot more detail there, but the employer does have to give 14 days notice usually that surveillance will take place, inform workers of the type of surveillance, the length, the start, the date and the purpose. In the ACT in particular there are specific provisions about what you do with that data once the workers are surveilled, what happens to that data and what protections are in place. New South Wales is a little bit vague on those points, but the ACT has some really specific provisions that could be beneficial in the development of the Victorian legislation. ACT also has consultation provisions, so if the employer is going to introduce workplace surveillance technologies, there is a provision in the ACT legislation that says the employer has to consult with workers about the introduction of these technologies. In both jurisdictions covert or secretive surveillance is also prohibited, which is very important, and we do not have that prohibition in this state.

**Dylan WIGHT**: So would that extend to maybe a situation in a business where a private investigator is used for when somebody is taking sick leave or when they are not fit for work et cetera?

**Jacqueline MEREDITH**: Yes. There is a complete prohibition on covert surveillance unless there is an order of a court or a tribunal. If you have a court order or a tribunal order which allows it, that is going to be an exception. But there is also a specific provision that says we have to take into account the worker's right to privacy here. If the covert surveillance is going to unduly interfere with the right to privacy, then the court is not supposed to grant that covert surveillance order.

There are definitely positives from the legislation in those other jurisdictions. Like we mentioned before, however, we do not think they are the perfect model for a best practice approach in Victoria. There are also limitations. Yes, while the approach to covert surveillance is beneficial, when we look at overt surveillance or open surveillance, there are really no limitations. So the approach in those other jurisdictions is really not that much better than the current approach in Victoria for overt or open surveillance. There are no restrictions. The employer does not have to have a legitimate purpose. They do not have to do the surveillance by the least intrusive means possible. As long as there is notice and disclosure, that is going to be sufficient.

**Dylan WIGHT**: The last thing I was going to add, and I think you have just answered my question—there is obviously consultation within the ACT model but not within the New South Wales model. I am assuming there is no real capacity there to dispute it, I guess—you get told and it is what it is.

**Jacqueline MEREDITH**: Exactly. And there was a 2022 New South Wales parliamentary select committee which basically criticised the New South Wales legislation for this exact same issue. As long as the employer notifies the worker this will take place, there is no mechanism to dispute it or negotiate it.

**Dylan WIGHT**: Thank you.

**The CHAIR**: I might just build on that. In your submission also you talked about the European Union. Is there something we can learn from that where you are seeing some best practice?

**Jacqueline MEREDITH**: Yes. The European *General Data Protection Regulation* was implemented in 2018. I think one of the key things to take away from that is that consent is very rarely going to be an appropriate basis upon which surveillance can take place, so it is very much contrary to the current Victorian approach. Like we said before, in Victoria if the worker consents, explicitly or implicitly, that is generally going

to be sufficient. Under the European *General Data Protection Regulation* there is a recognition that especially in the employment relationship consent is not freely given. So consent is very rarely under that regulation going to be appropriate. The regulation very much uses a legitimate purpose type approach. That is the proportionality-type approach I was talking about previously. The employer will have to demonstrate that they have this legitimate interest. Then within the European Union it is open to the different countries to develop more specific regulations on workplace surveillance, so we have countries like Finland which have said there has going to be a strict necessity requirement, so there has to be a strict necessity for this type of workplace surveillance. Even if a worker consents, that is irrelevant. As long as there is a strict necessity, that is what they have to show, and consent is not going to change that.

**The CHAIR**: And is that necessity mainly—is there an example where it is about safety?

**Jacqueline MEREDITH**: Yes, so the protection of health and safety and protection of property.

**The CHAIR**: Okay. We have got a few more minutes. Kim, do you want to ask anything?

**Kim O'KEEFFE**: Sure. It is great having you both here, and Jacqueline, with your background in law, it is really helpful. One of the questions we have got is: as some submissions prefer the development of best practice guidelines on workplace surveillance rather than law reform, what are the pros and cons of this approach? You can imagine some of them are not keen to have this heightened. I am interested to see what the pros and cons would be of just having practice guidelines in preference to law reform.

**Jacqueline MEREDITH**: We would say workplace-specific legislation dealing with workplace surveillance is the preferred approach. Best practice guidelines: is an employer really going to stick to those guidelines unless we have got some type of enforcement agency which is monitoring those guidelines, making sure that they are being implemented and taking action if they are not implemented, which is usually not something that is going to be the case? We would advocate for actual workplace surveillance legislation with a separate authority that is enforcing that legislation.

**Kim O'KEEFFE**: I suppose, following on from that, some people are quite nervous about that being enforced, having law reform put into their business, into their workplace. They are probably looking at lots of reasons why they are concerned about that. Do you have any reason why you think that maybe that concern may be raised?

**Jacqueline MEREDITH**: I think work health and safety could be an issue here. I know that some businesses would say, 'Workplace surveillance is actually useful for us to help detect work health and safety risks. We have a positive duty to eliminate sexual harassment, we have duties under the Occupational Health and Safety Act to have a safe workplace and we kind of need these workplace surveillance devices to monitor the workplace to make sure there is no discriminatory or harassing conduct happening.' That can still exist under what we are advocating for in our submission, but it would be more under this kind of proportionality-type principle. So, yes, you can still monitor workers. We are not saying you have to completely prohibit workplace surveillance. You can still monitor workers, but it has to be for a legitimate purpose, it has to be proportionate and there have to be safeguards, so disclosing to the workers 'This is when the monitoring will start, this is the purpose of it and this is what's going to happen to your data' and consulting with workers prior to that happening. So long as there are safeguards in place, it can be done for a legitimate purpose.

**Peter HOLLAND**: I think that is the key thing—it is safeguards. We are trying to emphasise how fast things have moved in the last five years. It is actually putting in the safeguards. The equivalent is, like, electric cars—there is a difference in what they are going to impact the environment with, so we have to then put safeguards in. We are not looking at draconian measures; we are saying it is important that managers understand that there is a lot of information being gathered here. You need to understand why you are doing it, if you need to do it and how you are managing that information.

**Kim O'KEEFFE**: Good. Thank you.

**The CHAIR**: Anthony.

**Anthony CIANFLONE**: You were talking about the need potentially for an enforcement agency to oversee how such surveillance is implemented, monitored, stored and tracked in terms of data and workers rights. In that respect, do you see a role for WorkSafe potentially being in that space?

**Jacqueline MEREDITH**: Yes, definitely. That is the approach currently taken in the ACT. Whatever their equivalent is of WorkSafe Victoria, the inspectors for the workplace also have jurisdiction under workplace surveillance legislation, so they can come into the workplace, inspect and enforce the legislation when there has been a breach.

**Anthony CIANFLONE**: Is there much resistance, as far as you are aware, potentially from business sectors, small businesses who—

**Jacqueline MEREDITH**: I am not certain about that.

**Anthony CIANFLONE**: Okay. The other question I had was around AI, artificial intelligence. How do you see that playing out in terms of potential new laws in Victoria?

**Peter HOLLAND**: Again, the emphasis of the future, and if we are here in five years time we might just be talking about artificial intelligence. It is the rapid rate at which this is going. We could maybe project—again false information, the use in political campaigns, false speeches being made by people and stuff like that—but who knows what information is going to be out there? So it does not actually mean it might help business, because they have to monitor and surveil what they pick up so they are not picking up false information. With students, for example, we have a good example in ChatGPT: if it does not know what it is doing, it makes stuff up, but the students still get dragged to using it, and stuff like that. AI is a great one. Who knows where we are going to be? We might just have avatars of us in five years time coming in to talk. Who knows?

**Jacqueline MEREDITH**: I think also—maybe just very briefly on that point—because the technology is changing so quickly, we probably do not have any real sense of what type of workplace surveillance devices will be in place in five years or 10 years. So when legislation is drafted it would need to be quite broad in its definitions, maybe quite a technologically neutral type approach, so not giving specifics about specific types of devices and keeping in mind the fact that these devices are probably going to evolve and new devices will exist in the future.

**Peter HOLLAND**: The *Privacy Act 1988* predates the internet, and we know that we live off the internet. So, yes, I think that is a great point about AI: in five years time the legislation might be dated because it is specific.

**Anthony CIANFLONE**: But do the New South Wales and ACT pieces of legislation make provision at all, to any degree, for AI or not so much?

**Jacqueline MEREDITH**: No. They are quite specific in their definitions. Like the current Victorian framework, we have got a definition for 'optical device' or 'listening device' or 'tracking device'. I think in drafting legislation we kind of need a broader approach that is more technologically neutral.

**The CHAIR**: I am just mindful of time, but I really want to get to John's question, only because it will help us with setting up for the day and other witnesses. So I will let John have his question.

**John MULLAHY**: Yes. You mentioned about biometric data and things like that being tracked and organisations storing that type of data. I have got concerns that on a weekly, fortnightly or monthly basis we hear of corporations getting their systems hacked, with access to customer or client-facing data. What sort of risks do we have with regard to computer surveillance that are posed to the workers and employers?

**Peter HOLLAND**: Biometrics is an interesting one. I recently did a paper, and the key case in the world was in Queensland, where a worker refused to give his fingerprints and was sacked—and that was upheld. Thankfully it was overturned, but there is an issue here about how much information companies can and cannot take—biometrics, iris, all this. If that gets hacked, you cannot replace it. You can replace a PIN, but you cannot replace that data. That data can feed into false profiles of people and things like that. So, yes, as with the AI, that I think is a real concern for the next five years, the amount of biometric information that is being picked up.

I think the Australia Institute last week or so did a research paper on companies asking for blood tests during the recruitment and selection process. Again, as Jacqueline said, when you are in the process you do not want to not consent, and they found that they were being not continued through the recruitment process. A blood test is going to give you lots of information about somebody. These are real concerns. This is another frontier. Biometrics is another frontier; it might be the next committee we come and talk to you on. But again, I find it really worrying, the amount of information being picked up. There are checks and balances in the law for it, but a lot of companies do not understand it. The biggest companies in the country are being hacked.

**John MULLAHY**: I think the security of their systems is paramount, and—

**Peter HOLLAND**: Yes, that is right. That is it.

**John MULLAHY**: it is a weekly or daily thing.

**Peter HOLLAND**: Yes. I personally was hacked in one of those medical big companies, and we were no longer members. They had just kept all that data of ours. So, again, companies you move from and move to are picking up data from you and then holding it. It is another area for you to keep you busy.

**John MULLAHY**: That is an aspect of that. Would there be anywhere in this where we need to make them purge data over a period of time? If we gave them the ability for workplace surveillance, how long can they store it for? Would that be an aspect of legislation?

**Peter HOLLAND**: Oh, absolutely. I made a note about that—and what access do people have to know what information you are holding? I think if people had the ability to know that they can look at the data, the company will look at what data they are holding, where they are holding it and for how long and how they are going to destroy it. With ethics, when we do research we have a five-year limit and then we have to destroy the data. So how long is it being kept for?

**John MULLAHY**: If you are no longer an employee, should it be wiped on the way out the door?

**Peter HOLLAND**: Yes, absolutely.

**John MULLAHY**: As you take your box.

**Jacqueline MEREDITH**: Exactly. The ACT legislation does have a provision for that, where workers are entitled to request the data that is being held about them. Also, under the European approach they are very big on transparency and giving workers access to that type of information. Like Peter said, if the employer knows that the worker is going to have access to this data, that might change their thinking.

**Peter HOLLAND**: Yes. And that goes back to that key point I said at the start, which is that the students I have taught who are HR managers said they access data because they can. For example, when they are recruiting someone they will go and have a look at their website and all that. I said, 'Isn't that a bit inappropriate?' And they go, 'Yes, but we can do it.' If HR know they cannot do it, then they might be more about managing their own boundaries, like the panopticon. They are going to manage themselves by saying, 'I could get that information, but that could get me into trouble and I don't really need that information.' So they are the issues as well, but AI and biometrics are the next wave of this.

**The CHAIR**: Thank you. I think we could keep asking a lot of questions.

**Peter HOLLAND**: You are parliamentarians. We are academics. We could talk forever.

**The CHAIR**: Yes. We could talk forever. And the thing is, you have set us up really perfectly for the start of our hearing. But if there is anything that you think has not been raised today or questions that you would like to give us further information on, we certainly can accept that further information. If there is something that—

**Peter HOLLAND**: Yes. I can certainly send you something on the biometrics.

**The CHAIR**: Yes. That would be wonderful. Thank you.

**Peter HOLLAND**: That is a really scary one, because the initial results were that the courts have said 'Yes, you can take people's biometric information even though they don't want you to.' And this was simply just to clock in and clock out. If we are going to let that happen, where does it stop?

**The CHAIR**: Yes. Thank you. Thank you so much.

**Peter HOLLAND**: So yes, I can pass that on to you—or is it to Kerryn?

**The CHAIR**: Yes. It can come to Kerryn and our secretariat. Thank you.

**Peter HOLLAND**: Okay. Well, I hope we have helped you.

**The CHAIR**: You have. It has been an excellent conversation.

**Peter HOLLAND**: Lovely. Thank you very much.

**Kim O'KEEFFE**: And if there is anything that we did not get to—I notice you have a lot of notes there. If there is anything we did not touch on today, please reach out, because you have done a lot of work there. Thank you, Jacqueline.

**Jacqueline MEREDITH**: Yes. Thank you.

**Peter HOLLAND**: Yes.

**The CHAIR**: Thank you so much.

**Witnesses withdrew.**