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

Sean Morrison, Victorian Information Commissioner, and

Rachel Dixon, Privacy and Data Protection Deputy Commissioner, Office of the Victorian Information Commissioner.

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 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 also be published on the Committee's website.

Thank you for your time today. I really appreciate you being here. I will introduce the Committee. Then we might get you to make some opening statements about your submission, and then we will head into some questions. I am Alison, the Chair, Member for Bellarine.

Kim O'KEEFFE: Good morning. Kim O'Keeffe, Member for Shepparton, and I am Deputy Chair. Welcome.

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: We might, if you could, have you talk for 5 minutes to your submission to give us a bit of background, and then we will head straight into some questions.

Sean MORRISON: Thanks. I assume no introductions are needed. Do you know who we are?

The CHAIR: Got you there, yes.

Sean MORRISON: I will just open by reading a short statement. It will be less than 5 minutes. Our statement expands on some of the points made in our submission and notes some of the primary concerns that may be of interest to the Committee. Obviously OVIC has oversight of the Freedom of Information Act and the Privacy and Data Protection Act, and surveillance activities by their nature we say are incursions on the privacy of those being surveilled. Whether this incursion constitutes a breach of that person's privacy depends on whether the act or surveillance pursues a legitimate objective and is reasonable, necessary and proportionate to achieving that objective.

There are many reasons why an employer may wish to surveil employees, such as workplace health and safety, but in any case, surveillance is an asymmetrical transfer of information and affects the balance of power between employees and employers. For this reason OVIC has recommended that the Committee consider whether a new principles-based regulatory framework should be developed to address the high privacy risks of workplace surveillance activities. That legislation, we would say, would probably be better implemented or merged into the current privacy framework than having specific standalone legislation that competes with the overarching privacy obligations of the public sector.

Some of the risks of workplace surveillance are overcollection, function creep and a gradual erosion of security controls. Workplace surveillance means an employer has collected more information relating to an employee than would have been collected if the activity did not take place. Overcollection and indefinite retention place the personal information of employees unnecessarily at risk. There is also a concern that employers use the collected information for a reason other than the primary purpose for which the surveillance activity gathered it. Function creep over time and through mere availability impacts employees' personal information where it is used for a purpose other than the purpose for which it was collected. The risk of function creep is a significant concern because it is gradual and hard to detect but has serious consequences for employees, in some cases putting their health and safety at risk. In these situations we see that there are principles and best practice when these activities occur but over time there is no audit function. People lose track of the data and you get this function creep if someone who owned the program and is a champion for privacy moves on and there are no proper procedures.

We are also concerned with the security controls on the collected data. For example, who has access to the footage for CCTV and how, when and in what circumstances may it be used? The controls must be audited regularly, particularly as an organisation grows. We have seen this with OVIC with some of the situations we have had. As I said before, there are best intentions but there is no audit program and no risk framework to this information.

Rapid developments in technology are making AI surveillance and biometric surveillance more commonplace. Firstly, biometric information must be afforded greater protections under the Privacy and Data Protection Act. It should be defined as sensitive information in line with the federal Privacy Act because the compromise of an individual's biometrics can have devastating and ongoing identity fraud consequences. The previously appearing witnesses spoke about that. It is irreplaceable; it is one and done. AI may make surveilling employees more efficient; however, the inherent biases of AI software can affect the legitimacy and accuracy of the surveillance. For example, an AI used to analyse performance data may prejudice some employees over others based on characteristics unrelated to their performance. It is also difficult to explain decisions made by AI models, even for those who develop them. Discrimination due to inherent AI biases may go undetected and unfairly affect employees of an organisation.

To negate unlawful and unethical workplace surveillance and minimise the risks to organisations and employees, the Committee should also consider a positive obligation on employers to demonstrate prior to its commencement that a high privacy risk workplace surveillance activity pursues a legitimate objective and is reasonable, necessary and proportionate. I cannot speak to who will appear, but I think you will hear these words a lot—that is, 'reasonable, necessary and proportionate'.

We also say that this work should include both a privacy impact assessment and a security risk assessment, and any new framework must consider accessibility of surveillance data. We oversee the *Freedom of Information Act*, and people should have access to this information, especially if it is being used for a disciplinary or lawful purpose against them. We say this is a fundamental protection in the balance of power between employers and employees.

Finally, OVIC believe a principles-based framework is required to keep pace with inevitable and rapid technological change. We administer the information privacy principles, which were developed in the 90s, and they are still highly relevant to today's information environment because they regulate through fundamental principles rather than regulating specific contexts.

I think in my last 30 seconds I would say that we may follow up with a further submission, having reread our submission, to note again that we think potentially standalone legislation may confuse. While it may be helpful, when you have different competing legislation, it is quite difficult for employers and for individuals. We also say that we oversee part 4 of the Privacy and Data Protection Act and that concerns data breaches, but some organisations are not covered by that, just by the drafting of the act. If they are a public sector organisation, we oversee them for privacy. But for data breaches hospitals, universities and courts in certain functions are all out. We would say that they should be covered under part 4 so that we have oversight of data breaches in relation to workplace surveillance.

The other thing I would add is that currently we are the regulator of last resort for workplace surveillance, in effect that if it is a breach of the information privacy principles, they come to OVIC. That is it for our opening statement.

The CHAIR: Thank you. That is really comprehensive. Much appreciated. Dylan, I might go to you first for questions.

Dylan WIGHT: Thank you. Thanks, Sean, and thanks, Rachel. You did touch on this within your statement, but I think it is important to elaborate on. We have already heard this morning that there are many cases where workers are being surveilled without them knowing, and some cases where they do. Can you just elaborate on people's access to that data or access to that surveillance that is being undertaken of them? Is it able to be FOI-ed? If it is not, how do we address that in the future? I think that is a really important fundamental point. If the response is that it is not able to be FOI-ed or accessed, that is something that we will need to look at in the future, I guess.

Sean MORRISON: Well, it is subject to the Freedom of Information Act. I would say in general there would be a resistance to providing that information. It would be assessed, but typically exemptions may apply for law enforcement or when it contains the personal information of other individuals and it cannot be pixelated or edited. It is subject to the Act, but there are a number of exemptions that could apply. Typically the justification may be that you could subpoena that footage et cetera, but when we get into quasilegal processes like workplace discipline, we would argue that there needs to be a clearer channel for people to have access to that information.

Dylan WIGHT: Okay. That is really sort of where I was going; I understand the police surveillance and things of that nature, but is there streamlining that needs to occur or is there change that needs to occur to make sure that that sort of request does not get caught up in an exemption?

Sean MORRISON: Agencies can choose not to apply that or could have better technology to provide that information. I note that the Integrity and Oversight Committee is reviewing the Freedom of Information Act, so it may be something you refer over to them. It could take place now, but if there was something in legislation that potentially pushed that to happen—maybe it was a prerogative right subject to some exemptions, like health and safety, security concerns et cetera—so it was flipped to being mandatory disclosure rather than a discretion.

The CHAIR: Kim.

Kim O'KEEFFE: Thank you. One of my questions is: to what extent do VPS employees contact your office about workplace surveillance, and what are their most common concerns? They are quite broad questions.

Rachel DIXON: They are. We do have some complaints that will come to us related to certain things, and they usually do go to a misunderstanding between the employer and the employee about what the proportionality piece is—for example, where employers are not clear about the purposes for which the information will be used and what the lawful basis for that is. Without confusing the consent issue, consent can quite often be quite easily bypassed, because it is kind of like, 'Well, if you want to work here, this is the thing,' which is not really informed consent. But that is actually not where I think we see the majority of the problems. Where we see the majority of the problems goes to Sean's opening statement, which is that once the tool is there, unless management has been very explicit with the employees about the use case—'Why are we doing this? What is the use case? What is the problem we're trying to solve?'—first of all, you cannot say that the consent is then reasonable, but secondly, you cannot then see whether the controls are being appropriately applied.

To give you an example, we may appear slightly hypocritical, but we actually run CCTV in our own workplace. We do that because—now, I, mercifully, have no role in FOI and I am very pleased about that, but I do have a role in privacy and security—we hold, as the information regulator, an enormous volume of highly sensitive material, be it cabinet documents, be it privacy cases. We also hold a lot of Victoria Police data because we regulate Victoria Police. For that reason we felt that it was very important to know whether there were circumstances in which that data might be exposed. So we run CCTV cameras; we have prominent signage. We introduced that policy to the staff very carefully, and we have a very tight access control regime. It can only be accessed by two people in concert—never a single person; that is inappropriate access—and only in response to an identified incident.

For example, we had a building worker who managed to bypass—well, set off our alarm, actually; we run our own alarm service—and they set off an alarm and they were wandering around the premises. We wanted to see what they had looked at. We were able to review the footage and see that they had not in fact been exposed to anything sensitive. That was the full extent of the access. We would never access that material for other purposes. We may need to adjust our policy to take account of, for example, if there was a workplace injury. But when we introduced the policy, we did not include that in our use policy.

So these are the sorts of things you then need to evolve and talk to your staff about. This is a high-management overhead, so to employers who are thinking that this is a nice Swiss army knife to solve a lot of workplace problems: no, it actually creates a very big overhead for you if you want to be compliant with the Privacy Act

consistently. And when you have got new people being onboarded you have to go through that all over again. I think those are big considerations. So it is not as attractive as it sounds.

Sean MORRISON: And just on the themes, it is the standard ones: the use of CCTV; dual SIMs on mobile phones; how employers can access, if it is BYOD, bring your own device, if the employer's software is on there, what monitoring is going on; and requirements for staff to have location services on. Work from home has opened up—we have not got a flood of complaints, but it is going to be the next frontier, as the previous witnesses spoke about.

Anthony CIANFLONE: Thank you. That brings me to the question I wanted to ask you around work from home. I like the way you summarise it in your submission, where you say:

> Privacy is central to an individual's right to live a full, free and dignified life, without fear of coercion or persecution for who they are or what they choose to believe. In this way, privacy is closely interlinked with other human rights such as the freedom of conscience, thought and belief, freedom of expression and freedom of association.
>
> Any form of surveillance may interfere with this right to privacy.

In terms of working from home, it is really where the two come to a head in that sense. How are you experiencing it from your office's point of view around the impact on privacy of VPS workers in particular, having worked from home, and what steps can we take as part of this inquiry's work to reform legislation to make provision accordingly for those needs or those experiences?

Rachel DIXON: I was around during COVID, so I can talk to how we implemented some of these things. We had two concerns at the outbreak of the COVID epidemic. We did not have a concern around staff productivity, interestingly enough, but we have a relatively small workforce, we know them all very well and it is much easier to manage in that kind of context. We were concerned about a couple of things. One was obviously that people had a safe working environment. That was important. We were not surveilling them to find that out, but we did deliver them the equipment that they needed to make sure that that was available to them. It was their responsibility to tell us that they were then setting it up appropriately and had an ergonomic chair and all of those sorts of things. We put the onus on them to tell us. We did that. We managed that reasonably well.

We do not monitor the amount of time people are online. That is not who we are as an organisation. What we do monitor is whether we are getting through the case load that we have, and then that is something we discuss with the managers of the staff because it is ultimately their job to do that. But we are not monitoring individual staff. All we are looking at is how many privacy cases we cleared, how many FOI cases we cleared. Interestingly enough, our productivity went up during the pandemic, which was the result of people not having to spend 2 hours a day commuting, which I am sure everybody was very fond of.

Sean MORRISON: That is a different committee.

Rachel DIXON: Anyway, the further piece to that, though, obviously then is that we did have to have conversations with the staff around the security element. We did not want to watch them doing things. That was not the purpose of things. But we needed to be sure that they understood the confidentiality of pieces—to not be on conference calls where other people could hear the content of those calls, which for some people living in one-bedroom apartments was a considerable challenge. And we obviously do not want to intrude on the private lives of the people who are sharing that environment with them either. So the only way to manage that in this situation is to just work with your staff to understand what their constraints are and then whether you can reschedule things or move things around. Not all work workplaces will have that flexibility. We are a very small workplace. But you do have to be conscious of not just your workforce but the families and friends and housemates of the people that are working for you.

Sean MORRISON: I think it is the tension. The thing you will hear about is the tension between employers—that is, they obviously have occupational health and safety obligations and confidentiality obligations to the right to privacy—them butting together. So how I would see it working is—it has to be a case-by-case basis. The employer has to do the analysis, coming back to what is proportionate, what is necessary. If you are dealing with data of the highest information classification, say it is related to terrorism offences, is working from home appropriate? I do not want privacy to be used as a wedge to have that conversation of bringing people back into the office, but I think it is. There needs to be legislation that provides

broad principles, but it needs to be applied to the facts and circumstances rather than, 'We are just going to do X because it's convenient for us.'

Rachel DIXON: The exemptions around IPP 2, which is use and disclosure—where you have exemptions for particular things, that is where some of the stuff can get tricky. You might say, 'Well, surely if you have got some sort of surveillance tech running on your workers, you should be able to disclose that in the event that it is an OH&S situation or that it is a criminal thing.' We would say again you get to the proportionality—'How serious is this?'—but also have you communicated to your staff that you will be doing this? Because even though you may have the legal right to do it, not informing your staff that this is one of the conditions in which that will be done is essentially a breach of the employer–employee trust relationship, which is corrosive to good management, really.

Anthony CIANFLONE: This is bread and butter for OVIC, obviously. You deal with data and privacy every single day, and those mature ways you have handled those examples you gave around CCTV as well and working from home are great case studies and examples. I guess the challenge for us is to find out how to make those recommendations apply more broadly, and obviously your evidence will be important in considering that.

The CHAIR: John.

John MULLAHY: The more broad aspect that I am going to come up with is essentially the Privacy Act, the Commonwealth legislation, exempts small businesses that have an annual turnover of less than $3 million. The issue is that with the technology that we have these days, businesses under $3 million are not going to be surveilling everyone. How do we protect those workers and the employers who are having good relationships with their employees in these instances? Do we need to have that aspect when we develop legislation here in Victoria?

Sean MORRISON: Well, we hope the federal privacy reforms get up and then potentially they are covered. It is not under our patch, but we are seeing more issues with this distinction between under $3 million and over, especially that $3 million is not a lot of money now for a lot of businesses.

John MULLAHY: That is 20 staff.

Sean MORRISON: But I think if I could take it one step back, you have got two concerns: you theoretically could have public sector legislation or oversight and then you have got the private sector, and you have got the federal sphere and the Victorian sphere, so you could make laws in Victoria that would cut across that—and I believe you could—that just apply to all businesses whether you are public sector or private sector. I think a framework that applies to all, but then you get into the issue of dual regulators. OVIC is not fishing for more responsibility. We will note that any responsibility, if it could please come with a successful budget bid—just put that on the record. But it causes confusion again when you have dual regulatory and enforcement schemes. So that would be the issue: who regulates.

Dylan WIGHT: Can I just follow on from that really quickly? Witnesses prior spoke about separate legislation with a separate regulator. I know that you guys have a sort of different opinion to that. What would you suggest or who would you suggest as a regulator? What framework do you suggest there to enforce and regulate, whether it is separate legislation or some amendments?

Sean MORRISON: We would suggest OVIC. We are not the self-licking ice cream, it is just that we have the relevant experts in OVIC at the moment. We deal with these things. What is the difference between a workplace surveillance breach, if it is a data breach, to another data breach? We have put in a submission to the IOC saying that in Victoria we have a distinction between health information and personal information. We have asked that they all come under our umbrella of responsibilities, and the health complaints commissioner has agreed with that. So you are potentially seeing this conglomeration coming together, one regulator. It is a data breach, what is different to a workplace surveillance data breach? Would that confuse it? Would another regulator have different standards, a different approach? If you think about it from the consumer's or individual's point of view, they phone OVIC, we say, 'Sorry, is it personal information? Yes, but if it's workplace surveillance, you have to call WorkSafe.' They are all ideas. I think, reading the submissions, everyone is saying that there is a patchwork of legislation that is not fit for purpose. I am not criticising anyone.

Rachel DIXON: If I can just briefly add to that, a really important component of any of this stuff is the education you provide to managers and staff. To the extent that the framework is more complicated and it involves multiple regulators, it just gets much harder to explain. And whose responsibility is it to explain it properly? Well, if you have got one regulator who is explaining 90 per cent of it really, really well but the 10 per cent that belongs to the other regulator is really poorly explained, that does not help anybody. So I think that is a really crucial thing.

I will say that it has not helped in Australia that while the OAIC and OVIC work very closely together and we work with the other state regulators insofar as we collaborate and talk regularly—in a perfect world I would not start a country from a federation because it is constitutionally very complex. But we have the issue where—and this is relevant in data breaches—if a private sector business is actually operating under state contract, then they actually fall under our Act, not the OAIC's Act, and private sector companies are not always aware of this. Toll road operators, for example, think that they are private companies—well, not when they are operating a toll road they are not, because it is under a state concession. So those sorts of things are complicated enough without throwing additional regulators into the mix. It is already a very difficult field to manage. And it is the education piece that is absolutely crucial to preventing the problems in the first place.

The CHAIR: Did you have anything to follow up on yours?

John MULLAHY: No, that is okay.

The CHAIR: I just wanted to touch on biometrics information. I suppose it is a new frontier, as it has been described today. Do you have any suggestions or advice on how that biometric data could be better protected in terms of that privacy for a worker?

Sean MORRISON: We say that the first fix would be making it sensitive information under the Privacy and Data Protection Act, because then effectively it has to be—there are some carve-outs—collected by consent. But we think there should be further and better protections around biometrics, and that comes into potentially a privacy impact assessment being done and a security impact assessment being done, all of these things. It is the next step up from personal and sensitive information—it is the top of the tree for us. There need to be tighter controls. There need to be better information security practices. Apart from consent, there needs to be this proportionality aspect to it.

Rachel DIXON: And there needs to be some resourcing applied to actually then deal with the consequences. One of the things that I think was raised in a question to a previous witness was data breaches. The problem is that contractually most state contracts, for example, contain clauses that say that contractors will delete the information, and under the IPPs they have to delete it when it is no longer required. If the employee has left, you do not really need to hold biometric information on them. But there is a cost to an employer of having somebody go into the system and delete all the biometrics that are associated with those people, so a lot of businesses do not do it, but you only find that out when the breach happens.

It was not workplace related, but there was a data breach last year at a company under a state contract that held a lot of personal information of Victorians that they had not deleted ever despite their contracts saying that they were supposed to. So unless you actually have some regulator who is going to do some random audits of things like that, you are never going to know. It is all great to have a piece of legislation that says everybody will delete these biometrics after, but you have to resource that or it is not going to be effective.

The CHAIR: Can I just confirm: if an employee leaves a workplace, under most circumstances there is a contractual obligation to delete?

Rachel DIXON: Well, what would you need biometrics for?

The CHAIR: But is there a law to state –

Rachel DIXON: IPP4 is very clear that information should be discarded when it is longer needed. There are PROV rules around the preservation of documents that apply, and we obviously would collaborate in producing resources together with PROV around some of these sorts of things. But if you are not working there anymore, why does your employer need your biometrics? You are not going to get access to their building anymore, but if you did get access to their building, that would be a security breach. You can see that there is a clear interest.

The one caveat I would make is that there are also smart ways of doing biometrics and dumb ways of doing biometrics. The dumb way is you just capture the biometric data and it is stored, like a fingerprint or something, and you can see it there. That is dumb because in the event of a breach everyone sees it. Most modern biometrics systems will encrypt that information in some way. I think our submission talks to you about this: your phone biometric is essentially configured twice through the device ID. It is a hash that is combined with your device and your face—not the actual picture of your face, but the mathematical representation—and the account that you have got. If any one of those three things does not match, you cannot reverse-engineer it. It is why, if you have got an iPhone, when you get a new iPhone you have to re-enrol your face, right, because your old face does not work anymore because it is a different device. That is a better way.

A member interjected.

Rachel DIXON: Yes, I know. You will have to re-enrol yourself—you will. I am not endorsing a particular technology, I am just saying that there are—but again, all of these things cost money. The other piece about biometrics is that while they seem super convenient, they are often not proportionate to the actual problem you are trying to solve. There are lots of vendors out there who want to see the Swiss Army knife of facial recognition will solve this problem for you. Melbourne University held a little symposium late last year where they began the session with various facial recognition technology vendors starting with all of the wonderful things they could do. I think you are seeing it now with 'Unlock your supermarket trolley' or whatever 'with your face'—please do not do that.

The problem with these things is that over time you are gradually creating essentially the equivalent of a surveillance culture, which, as I think our submission makes clear, is not conducive to a sense of being a person in the world, the philosophical kind of independence that you have to proceed unmolested down a street or through a supermarket or any of those sorts of things—little by little, so proportionality is really crucial. I think Sean's point about making it 'sensitive information' will help to limit the ability of organisations to do some of that, because they have to have specifics, you know: why is this proportionate? And if it is sensitive information, then they do have to have consent for it, and that consent should be freely given.

The CHAIR: Thank you. Thank you so much for your time today. If there is anything further you would like to add or pass on to the Committee to review, we are more than happy to accept that as well.

Sean MORRISON: Definitely, we will send something through. And we will listen, and if there is anything that comes up with the other appearances, we will make a note for you as well.

The CHAIR: Wonderful. Thank you for your time today. We really appreciate it.

Witnesses withdrew.