T R A N S C R I P T

LEGISLATIVE ASSEMBLY ECONOMY AND INFRASTRUCTURE COMMITTEE

Inquiry into workplace surveillance

East Melbourne – Monday 23 September 2024

(via videoconference)

MEMBERS

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

WITNESSES

Jody Wright, Chief Executive Officer, and

Amy Elliott, Chairperson, Investigations Sector, Institute of Mercantile Agents.

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

All evidence given today is being recorded by Hansard and broadcast live on the Parliament's website.

While all evidence taken by the Committee is protected by parliamentary privilege, comments repeated outside 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.

Thank you so much, Amy and Jody, for coming today to help us unpick a little bit more about your industry and help us with this inquiry. I am happy for you to have a few minutes, maybe 3 or 4 minutes, if you want to give a bit of background or talk a little bit more about what you are seeing, and then we will jump straight into some questions.

Jody WRIGHT: Thank you for having us appear today. Just some background in relation to me and the Institute of Mercantile Agents. I am Jody Wright, and I am the current CEO of the Institute of Mercantile Agents. I commenced in this role in February 2024, succeeding Alan Harries, who was the former CEO and was the CEO for approximately 26 years. The Institute of Mercantile Agents was established in 1961, so we have been around for a very long time. We represent investigators, collectors, process servers and repossession agents throughout Australia. We are committed to ethics, compliance and best practice across the industry, including the investigation industry.

The IMA promotes the interests of members through advocacy, education, support and collaboration. We empower our members to excel in their professions and uphold the highest standards of integrity and professionalism. The IMA is also an approved security industry association in Queensland pursuant to the Security Providers Act. We also operate an approved bonding scheme for Western Australia in accordance with the WA Debt Collectors Licensing Act. Now, we are actually not an approved industry association in Victoria, but I am aware that there are several associations that represent investigators in Victoria who actually are approved security providers pursuant to the legislation in Victoria.

As detailed in our submission, which obviously I am not going to run through—everyone would have read that—we do support the Committee's inquiry and the terms of reference. The input that was provided by the IMA was actually provided on the basis that the association represents investigators throughout Australia who might actually be retained by employers, whether in the private sector or the public sector, to undertake workplace surveillance activities. Generally those activities that our members do participate in are done outside the place of work, so they are not going in there and doing surveillance inside the workplace or installing cameras inside the workplace.

Pursuant to the Victorian licensing legislation, as I said before, investigators are required to be members of an approved association. Although there is self-regulation in terms of specific guidelines or regulatory requirements that I guess govern the way that an investigator carries out their activities or the way that they conduct themselves when they are conducting those investigations, I certainly know in terms of the IMA that our members are required to sign a code of conduct and a code of ethics which actually determine how they do operate, making sure that they are compliant with whatever legislation, regulations, code of conduct or guidelines are applicable to them. I cannot speak for other associations in Victoria, but I would assume that the approved associations in Victoria have similar codes of conduct and codes of ethics that their members are required to follow. So even though there is not a fallback position in terms of regulatory guidance or regulatory repercussions if there is a breach by an investigator, there is certainly that fallback within the associations. The associations have power essentially. I know the IMA does. As I said, I cannot speak for other associations, but we do have the power to suspend or cancel their membership if there is a significant breach of a code of conduct or code of ethics. Amy, I do not know if there is anything else that you would like to add there.

Amy ELLIOTT: Yes. There are different organisations throughout Australia that help regulate private investigators with their own codes of conduct and their own ethical training. I know that in the state of New South Wales we have got the security licensing and enforcement directorate, which is overseen by the New South Wales police force, which allows us to get that licensing. They have really cracked down in the last six to

12 months on private investigators to make sure they are abiding by conduct, and as a result they will remove their licence, and they also now get fines. Then we have also got the naming and shaming, which has just come out in the last three months through the New South Wales police force. They are on Facebook and things like that, on their own pages, to keep us accountable. Obviously different states vary, but we have all got the same things. As Jody said, with the code of conduct, most of us are aware of it and are encouraged to join an association.

The CHAIR: Okay. Thank you so much for that. You are bringing a very different perspective to this inquiry, which is actually fantastic, so thank you so much for that. John, we might go to you first for a question.

John MULLAHY: No worries. Thanks, Jody and Amy, for that introduction and also for your submission. I am just interested in how common or widespread it is for employers to request private investigation of one of their workers. And do these often lead to disciplinary action or dismissal?

Jody WRIGHT: Members generally engage on a minimal basis to surveil workers, because generally most of this would be done by WorkSafe Australia or WorkCover or whatever the situation may be. Generally the only time that an investigator will come in is if they are retained directly under a panel arrangement by that workers compensation provider. The times that surveillance might be conducted are in relation to allegations that have been made, whether it is against the employer or against the employee in relation to misconduct or similar types of situations or trademark infringements. It is quite rare. I reached out to some of our members in Victoria, who said that, yes, it is on a minimal basis. I am not sure in terms of other investigators who are members of other associations how much work they do in that sphere, but in terms of our members it is actually minimal.

John MULLAHY: Just as a follow-up, would there be any data of that being tracked centrally in a database by you guys, by a state body or anything like that?

Jody WRIGHT: No, it is not tracked by the IMA. We are not privy to the work that our members do. It would be tracked internally by the members. They would be knowing how many jobs they are doing on a monthly basis. There is no need to report that back to anyone at this point. There is not a regulatory requirement for them to do that. I guess in terms of the public sector, they would be keeping a record of that within their own internal records. Private sector employers are probably doing the same, and I would think that WorkSafe, if they are sending investigators out to do surveillance, would be tracking that in some form or another.

Amy ELLIOTT: Is it okay if I just jump in? I am a licensed private investigator in the state of New South Wales, but I also contract out to my colleagues in Victoria and across nationwide. So in terms of private investigation work with workplace surveillance, there are usually about two types. It is obviously done inside where the employer surveils them through the computer and things like that. That is when private investigators do not really jump in so much, unless they do forensics or that specialty to look at computer use or things outside the laptops, but with private investigators contracted out to look at, say, WorkSafe issues or workers comp, usually that is through a panel. And then you have got the small odd jobs here and there where it is outside of that scope. You know, if someone is doing sick leave and they are not supposed to be—they are actually not sick—then we can jump in and surveil them and watch them while they are at work, or people working from home, if people are stealing intellectual property or if they have stolen a car and they are refusing to bring it back. We do get those types of jobs. It is not in the majority. In terms of reporting back to and declaring it to your associations, we do not at all. We hold that information on our own databases, and sometimes we do not even have databases. We have got our CRM. Sometimes everything is held through Outlook. So there is no actual regulatory body that oversees how we use that data. We do not have that at all.

John MULLAHY: Thanks.

The CHAIR: Thanks, John. Wayne.

Wayne FARNHAM: Thank you, Chair. Thank you for contributing to this. I suppose where I want to go is about accountability and how the private investigator is held accountable for the way they use surveillance technologies and their compliance with the relevant laws.

Jody WRIGHT: I can speak to that one. Thanks, Wayne. Generally—because there is a code of conduct that they do follow—the codes of conduct stipulate that investigators when they are carrying out their activities,

whether it is surveillance or it is factual investigation or whatever they are doing, they are doing it in accordance with whatever legislation and regulations apply within that area, so within that state. In dealing with data and surveillance methods and the gathering of that information of course they are complying with the Commonwealth Privacy Act and the Victorian privacy Act and principles. And they are also governed to a certain extent by the client's protocols and procedures. Often you will find particularly with government departments, if they are retaining investigators to surveil employees, they will have guidelines in place or a standard code of practice or procedures guides that investigators need to follow and strict compliance with that is required. You would find in that situation, if there is a panel arrangement in place, then the master service agreement within that government department—or say, for instance, even a private sector employer—will also have stipulations in there in relation to what the investigator can and cannot do in those circumstances.

Wayne FARNHAM: What happens if they breach it?

Jody WRIGHT: They are at risk of having their contract terminated, which means they will not be doing the work anymore, which is a significant problem for that investigation firm, particularly if that is their only source of income or a major source of their income.

Wayne FARNHAM: Thank you.

The CHAIR: Thank you. Anthony.

Anthony CIANFLONE: Thanks for appearing. My question, following on from Wayne, is around data handling and ownership of such data collected by private investigators. What actually happens to surveillance data if a private investigator does detect improper behaviour, and what happens to the data if the investigator does not detect any improper behaviour? The second part of that is: who actually ultimately owns that data, regardless of which way the investigation goes?

Jody WRIGHT: I can speak to those. There are a number of aspects to that question, so I will try and address each one individually. The data that is collected in a workplace investigation is supplied to the client, so it actually becomes the client's data. They have ownership over it; it is supplied back to them. It is normally done in the form of a report and the video footage obtained and things like that. Did you want me to speak to protection of that data as well in terms of the surveillance records that are held?

Anthony CIANFLONE: Yes, please.

Jody WRIGHT: Each respective agency would have their own data retention policy and privacy policy, I would assume, but of course I do not ask all of our members for copies of their data retention policies and their privacy policies. That would just be a nightmare, having to do that. But what we would expect is that they would have a data retention policy and privacy policy that would address how data is collected, stored and protected.

The data retention periods would also depend on circumstances. Generally it is recommended that the destruction of records held by investigators is actually done seven years after the last period of surveillance, and the reason it is seven years is for litigation purposes and also for insurance purposes if that data needs to be provided. Just say there is a claim made by the client against the investigator, the insurer is going to ask for copies of those records so it can determine what happened. That includes footage obtained.

We are seeing that investigators are increasingly using Microsoft 365 in relation to email, and Azure with encryption, and multifactor authentication is used along with the MS Authenticator app for any contracted investigators. Generally the way that investigators work is you will have a large agency who may have the contract with the client to undertake the surveillance work. They will then perhaps subcontract that work down the chain to third-party providers. In terms of accessing the information and storing it, they have multiple levels of multifactor authentication, ensuring that that is protected and it is not potentially breached or disclosed.

In relation to that, I just think that whatever guidelines the government implements will need to take into account the differing levels of investigation agencies and I guess their turnover. It is interesting because some bigger agencies may have what is called ISO 27001 certification, which is the standard that is followed in relation to the protection of data and personal information. There would be smaller players out there that just simply could not afford something to that extent, particularly in terms of the project management. Whatever is

introduced by the government, if anything is introduced, it is vital that the government takes into account the number of investigators out there, their size, their turnover and their potential capacity and ability to put a program like that in place.

What happens to surveillance data when the private investigator does not detect any improper activity? The data actually remains stored in the event that there are any issues that are raised later down the track by either the client or the subject of that investigation. They may still need access to that surveillance down the track. That works in favour of any of the parties involved, because they have all got the right to look at that surveillance data and interrogate the data and say, 'Hang on.' Or maybe there was a situation where that evidence is actually needed in relation to some other event that might be related to the reason for the surveillance being conducted.

The CHAIR: Amy.

Amy ELLIOTT: I was just going to add: the reality of private investigators—and this is mostly nationwide—is that most of them are ex police force, so they are semiretired. Most of them use either a Gmail account or an Outlook account, and most of their data is stored either in those Gmail or Outlook accounts but also in Google Docs, so that is how they transfer the large files of footage to the client. Most of them are subcontractors. They send it to the private investigation agency, then they upload it in their own CRM, which is protected by a multifactor authentication app and things like that. So the subbies, which are the majority of the investigators, are semiretired. Like Jody said, they cannot afford those protections, those securities. Most of them are using Gmail and Outlook and Google Docs drives. So they do not have that privacy, and it is really quite easy to hack, especially if they are sending that information just through a link. That link does not have an expiry, whereas other CRMs, like mine that I use, have expiries on those links and have double authentication. They do not pay for that, because most of them are semiretired and doing it just for a bit of cash on the side.

The CHAIR: Interesting. Thank you so much. I am so mindful of time. We did have more questions to ask, but I am so sorry, we have run out of time today. Thank you, though, for a different perspective really for this committee to consider. When we go to deliberate I am sure we will keep all these things in mind. Thank you so much for your time today.

Witnesses withdrew.