

Electronic surveillance in the workplace

Gathering evidence using mobile phones, photos, video footage and recorded conversations

The Deputy President in the Fair Work Commission has expressly stated that secret recordings in workplaces are:

“quite properly described as sneaky”, “abhorrent to ordinary persons dealing with each other in a proper fashion”, “deceptive and purposely misleading”, “its very sneakiness makes it abhorrent to ordinary persons”, “objectionable because one party is being deceptive and purposely misleading the other party”, “seriously wrong and inexcusable”, “a valid reason for dismissal”¹

As an investigator there are many factors to be mindful of when gathering electronic surveillance as evidence.

NB: Ensure you review the individual State based legislation in your operating area as there are variations between States.

As a general rule,

- Employers, employees and investigators must ensure compliance with the *Surveillance Devices Act 2007* NSW, the *Workplace Surveillance Act 2005* NSW, the federal *Telecommunications (Interception and Access) Act 1979* Commonwealth and relevant privacy legislation if surveillance is considered necessary in the workplace.
- Employers, investigators and HR Managers must exercise extreme caution if accepting or using footage or recordings, especially where an employee has produced files secretly taken of another employee at work. Generally, this practice is not acceptable.
- Procedural fairness and principles of natural justice still apply to investigations where surveillance footage or audio recordings are utilised.

Some other factors are listed below:

1. What is the law around electronic surveillance or monitoring legislation in the workplace that applies throughout Australia?

The laws governing the use of electronic surveillance or monitoring of employees is inconsistent between states and territories. Such legislation is device-specific and applies more broadly than in the workplace. New South Wales and the Australian Capital Territory are the only jurisdictions that have legislation **specifically relating to workplace surveillance**. Both sets of laws impose

¹ See *Lever v ANSTO* [2009] AIRC 784, *Schwenke v Silcar* [2013] FWC 4513, *Thomas v Newland Food Company Pty Ltd* [2013] FWC 8220 and *Thompson v John Holland* [2012] FWA 10363).

strict procedures for an employer to comply with around obtaining permission to perform covert surveillance in the workplace.

2. What is an electronic surveillance device?

There is no one definition of what an electronic surveillance device is. It is important to be aware that there are emerging technologies all of the time providing a broader range of surveillance options such as data surveillance. You will need to check the relevant governing legislation.

Electronic devices such as Mobile phones, iPads, laptops, tracking devices, drones and similar devices with cameras that can transmit, receive and/or record images, including videos are considered “optical surveillance devices” under State legislation. There are many apps that can be installed on computers and devices to visually observe or record activity.

A mobile phone and similar devices are a listening device if they can transmit, receive, and/or record audio. Under the *Surveillance Devices Act 2007* NSW, devices (other than hearing aids) capable of being used to overhear, record, monitor or listen to a conversations or words spoken in conversations are classified as listening devices.

3. Can a secret recording of a conversation be made in the workplace?

As a rule of thumb, recording private conversations is permissible provided that express or implied consent is obtained before the conversation takes place. A failure to obtain consent can be a breach of the law which may result in criminal punishment.

The *Surveillance Devices Act 2007* NSW only relates to private conversations. Private conversations in this context are conversations “carried on in circumstances that may reasonably be taken to indicate that any of the parties to the conversation desires it to be listened to only by themselves”. Private conversations do not include “conversation(s) carried on in circumstances in which the parties to the conversation ought reasonably to expect that the conversation may be overheard.” It an offence to knowingly record a private conversation regardless of whether they are a party in the conversation or not. It is also an offence to install, use or maintain a listening device to overhear, monitor or listen to a private conversation to which the person is not a party. The penalty for these offences is up to five years’ imprisonment and/or \$55,000.

4. Are there any exemptions to recording a conversation?

There are situations where possible exemptions can apply. If you are planning to record a conversation, legal advice should be sought before relying on any of the exemptions. These exemptions are outlined in the *Surveillance Devices Act 2007* NSW, and include:

- Recording a conversation you are part of, when the other principal parties to the conversation also consent to the recording;
- Using a listening device with a warrant or other legal authorisation;
- Using a listening device to record the refusal of a police interview;
- Police recording the operation of a Taser, or on body-worn video equipment;
- Unintentionally hearing a private conversation through a listening device;

- Recording a conversation you are a part of when it is reasonably necessary for the protection of your legal interests;
- Making a recording that is not made for the purpose of communicating or publishing the conversation, or making a report of the conversation; and
- When reasonably necessary in connection with an imminent threat of serious violence, substantial damage to property, or the commission of a serious narcotics offence.

5. Can a recording of a conversation be made over a phone line?

There are further prohibitions on recording phone conversations, teleconferences, or internet-based chats without the knowledge of people involved in the communication. Section 7 of the federal *Telecommunications (Interception and Access) Act 1979* Commonwealth prohibits a person intercepting or enabling a person to intercept a communication passing over a telecommunications system. Persons convicted can face 2 years imprisonment.

6. Can I use a recorded conversation in court proceedings?

Recordings that are obtained secretly or unlawfully may not be admissible as evidence in court proceedings. In regard to employment proceedings specifically, the Fair Work Commission has the discretion to accept such evidence, however breaches of relevant state surveillance legislation will attach a significant amount of weight to the decision as to whether the recording will be admitted into evidence.

7. Can employees be monitored in the workplace using a camera, computers or tracking devices?

The *Workplace Surveillance Act 2005* NSW prohibits covert surveillance in workplaces unless a “covert surveillance authorisation” is obtained from a Magistrate or if a prescribed exception applies e.g. in a casino, correctional centre, court, or for certain other law enforcement or security purposes.

Surveillance using cameras, computers or tracking devices can also be undertaken in situations where employees have been given 14 days’ notice in writing (in compliance with the Act).

Co-workers are also obliged to meet the legislative requirements and cannot make recordings of their colleagues unless they meet the requirements outlined above.

8. How does an employer get a covert surveillance authority to monitor employees in the work place?

Under Part 4 Division 2 Section 23 (1) of the *Workplace Surveillance Act 2005* NSW, an employer or their representative may apply to a Magistrate for the issue of an authority authorising covert surveillance of employees while at work. This surveillance is for the employer, for the purpose of establishing whether one or more particular employees are involved in any unlawful activity while at work.

9. Can I take photos or videos of people without their consent?

You cannot take photos or video from or on someone's private property, without their consent. Section 8 of the *Surveillance Devices Act 2007* NSW outlines limitations to using cameras to take images without consent. This restriction also applies to investigators unless you are exercising specific regulatory powers that authorises this type of conduct.

Photos and video footage cannot be taken in a workplace for investigation purposes or for monitoring or surveillance of employees without either adequate written notice under the *Workplace Surveillance Act 2005* NSW or authorisation from a Magistrate. The taking photos or videos when a person has a reasonable expectation of privacy is generally unlawful (for example in bathrooms and similar - voyeurism and indecency offences in the *Crimes Act 1900* NSW can apply).

10. Does privacy legislation relate to photos?

Federal privacy legislation protects personal information that is held, or collected for inclusion, in a "record".

A "record" is defined to include a photograph or other pictorial representation of a person. So, if an individual's identity is apparent or can reasonably be ascertained from a photograph, then the collection, use and disclosure of that image may be covered by the *Privacy Act 1988* Cth. This extends to video images as well as still photographs.

Images taken by a person acting on behalf of a state or territory agency are not covered by the *Privacy Act 1988* Cth (but NSW Public Sector agencies must adhere to the *Privacy and Personal Information Protection Act 1998* NSW when collecting, storing, sharing audio files, images or videos that contain personal information).