



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

Guide to Workplace Surveillance

AS AT SEPTEMBER 2019

How to use this guide

The laws regulating workplace surveillance vary between each State and Territory. Regardless of which law applies, employers should be mindful to implement best practice when it comes to maintaining privacy in the workplace.

The Fair Work Ombudsman publishes a Best Practice Guide located [here](#) that covers workplace privacy, general privacy principles and the protection of information.

The information in this guide is of a general nature. It is not intended to be a comprehensive summary of the law and should not be relied upon as legal advice.

For more information

Phone: 1800 RETAIL (738 245)



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

Table of Contents

Guide to Workplace Surveillance	1
As at June 2019	1
Table of Contents	2
Queensland	3
New South Wales	4
Victoria	8
South Australia	10
Western Australia	12
Tasmania	13
Northern Territory	15
Australian Capital Territory	17
Recording Telephone Conversations	21
Summary.....	22

Queensland

The *Invasion of Privacy Act 1971* (Qld) (**Act**) regulates the privacy of individuals in Queensland.

Can listening devices be installed in the workplace?

Listening devices must not be installed or used to overhear, record, monitor or listen to private conversations.

This will not apply where the person using the listening device is:

- a party to the private conversation;
- they unintentionally heard the conversation on a telephone; or
- for other law enforcement reasons.

What about optical surveillance?

Optical surveillance devices (for example, CCTV cameras) with audio recording capabilities may also be considered listening devices for the purposes of the Act.

The *Criminal Code Act 1899* (Qld) separately makes it an offence to record someone in a place where they would expect to be private, such as a bathroom or change room.

Are there restrictions on the use of material obtained through surveillance?

It is an offence to communicate or publish a private conversation, or a report of, or of the substance, meaning or purport of a private conversation. This applies irrespective of whether this information came to their attention directly or indirectly.

However, these restrictions do not apply where the communication or publication of the private conversation is made:

- to a party to the conversation or with the consent, express or implied of such a party; or
- in the course of legal proceedings (including before a Court or the Fair Work Commission).

Persons held responsible for breach of this provision may be liable for 2 years imprisonment or 40 penalty units.

What does this mean for my workplace?

Employers should not use install or use listening devices in the workplace.

While the use of optical surveillance devices is not significantly regulated in Queensland, employers should ensure that such devices do not record sound, and are not installed in bathrooms or change rooms.



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

New South Wales

The *Workplace Surveillance Act 2005* (NSW) (**Act**) prohibits unauthorised surveillance of employees using optical surveillance devices, computer surveillance devices and tracking devices.

What forms of surveillance are regulated?

The Act applies when an employee is “at work.” An employee is considered to be “at work” when an employee is:

- at the workplace of the employer (or a related corporation of the employer), whether or not the employee is actually performing work at the time; or
- any other place while performing work for the employer (or a related corporation of the employer).

The Act is specific to workplace surveillance, and it does not deal with the use of listening devices, including whether a camera is used to record sound, which are dealt with separately under the *Surveillance Devices Act 2007* (NSW).

In general, under the *Surveillance Devices Act 2007* (NSW) listening devices must not be knowingly installed, used or caused to be used or maintained, to overhear, record, monitor or listen to a private conversation, without the express or implied consent of each party to the conversation.

When may surveillance occur?

Optical, computer and tracking surveillance in the workplace must not commence without prior written notice to employees. Written notice expressly includes notice by email.

The notice, to be given at least 14 days before surveillance commences, must indicate:

1. the kind of surveillance to be carried out (optical, computer, tracking);
2. how the surveillance will be carried out;
3. when the surveillance will start;
4. whether the surveillance will be continuous or intermittent; and
5. whether the surveillance will be for a specified limited period or ongoing.

Employees who commence at the workplace within the 14 day period or after the commencement of surveillance must be notified of the surveillance prior to starting work.

An employee need not be provided with notice if the workplace is not that employee’s usual workplace.

Are there any other requirements?

Cameras used for surveillance must be clearly visible and each entrance to the premises must have clearly visible signs notifying people that they may be under surveillance.



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

A workplace utilising computer surveillance must have a relevant policy in place, which has been provided and explained to employees. If a vehicle or thing is subject to tracking surveillance, a notice should be clearly visible indicating that this is the case.

Are there restrictions on where surveillance devices can be located?

It is an offence to carry out surveillance in any change room, toilet facility or shower or other bathing facility at a workplace.

It is also an offence to carry out surveillance on an employee when an employee is not at work for the employer, for example using tracking surveillance outside of working hours.

Contravention of these requirements means the person may be liable for a maximum of 50 penalty units or 2 years imprisonment.

What are the restrictions on use and disclosure of surveillance material?

Records produced as a result of workplace surveillance must not be disclosed unless:

- the use or disclosure is for a legitimate purpose related to the employment of employees of the employer or the legitimate business activities or functions of the employer;
- disclosure is to a member or officer of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence;
- use or disclosure is for a purpose that is directly or indirectly related to the taking of civil or criminal proceedings;
- use or disclosure is reasonably believed to be necessary to avert an imminent threat of serious violence to persons or of substantial damage to property.

Contravention of this requirement means the person may be liable for a maximum of 20 penalty units or 2 years imprisonment.

Can covert surveillance be used in the workplace?

There are two circumstances in which covert surveillance can be used in the workplace.

Covert surveillance authority

If an employee is suspected of being involved in unlawful activities while at work for the employer, application may be made to a Magistrate for authorisation to conduct covert surveillance. An application for authority must contain the following information:

- a statement of the grounds the employer has for suspecting that a particular employee(s) is involved in unlawful activity, together with the names of those employees (unless it is not practicable to name them);
- a statement as to whether other managerial or investigative procedures have been undertaken to detect the unlawful activity and what has been their outcome;



National Retail
Association

GUIDE

- the names of the employees or (if it is not practicable to name them) a description of the group or class of employees who will regularly or ordinarily be the subject of the covert surveillance;
- a description of the premises, place, computer, vehicle or other thing that will regularly or ordinarily be the subject of the covert surveillance;
- a statement as to the kind of covert surveillance (camera, computer or tracking) that is proposed to be conducted;
- the dates and times during which the covert surveillance is proposed to be conducted;
- a statement as to whether any previous application for a covert surveillance authority has been made in respect of the proposed covert surveillance and a statement as to the results of the application and of any covert surveillance conducted under a covert surveillance authority issued as a result of the previous application;
- in the case of an application made by an employer's representative, verification acceptable to the Magistrate of the employer's authority for the person to act as an employer's representative for the purposes of the covert surveillance operation.

Such authorisation does not permit surveillance for the purposes of monitoring work performance and must not be carried out in any change room, toilet facility, or shower or bathing facility.

A covert surveillance authority has a maximum duration of 30 days, but may be cancelled before that time, and the surveillance operation must be overseen by a supervisor designated by the Magistrate. All surveillance records produced as a result of the covert surveillance must be destroyed within 3 months of the expiry of the authority.

If, as a consequence of the carrying out of covert surveillance of an employee, the employer takes, or proposes to take, any detrimental action against the employee, such as dismissal or disciplinary proceedings, the employer must, within a reasonable period after being requested to do so by the employee, give the employee access to any part of the surveillance record supplied to the employer that relates to the employee or the detrimental action.

A person must not make use of or disclose to another person surveillance information or a surveillance record knowing or having reasonable cause to suspect that the information has been obtained or the record made as a result, direct or indirect, of covert surveillance. Disclosure will be permitted where it is authorised by the covert surveillance officer. Where disclosure is not permitted, the employer may still be required to disclose the information for the purposes of law enforcement.

Surveillance for security of the workplace

Where this authority has not been obtained, there is a defence to prosecution where the surveillance of employees was carried out for the security of the workplace. In such a case, the employer must prove that:



National Retail
Association

GUIDE

- the surveillance was carried out solely for the purpose of ensuring the security of the workplace or persons in it and that surveillance of any employee was extrinsic to that purpose; and
- there was a real and significant likelihood of the security of the workplace or persons in it being jeopardised if covert surveillance was not carried out; and
- the employer notified employees at the workplace in writing of the intended surveillance and its purpose, before it was carried out.

Any surveillance material obtained in this manner that is unrelated to the security of the workplace and the persons in it is not to be admitted in evidence in any disciplinary or legal proceedings against the employee unless the desirability of admitting it outweighs the way in which it was obtained.

What does this mean for my workplace?

The legislation applicable to New South Wales provides specific guidance and requirements that employers must follow, especially with respect to covert surveillance.



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

Victoria

The *Surveillance Devices Act 1999* (Vic) (**Act**) regulates the installation and use of surveillance devices in Victoria.

Can I install and use a surveillance device in the workplace?

Listening and optical surveillance devices must not be knowingly installed, maintained or used to overhear, monitor, record or observe a private activity or private conversation to which the person is not a party, without the express or implied consent of each party to the conversation or activity.

A private conversation or private activity is one which is carried on in circumstances that may be reasonably taken to indicate that the parties desire it to be heard or observed only by themselves.

These prohibitions do not apply where the surveillance device is installed, used or maintained:

- in accordance with a warrant or emergency authorisation;
- in accordance with a law of the Commonwealth; or
- by a law enforcement officer that is not a party to the conversation or activity, if the at least one party to the conversation or activity consents to the monitoring or recording, which occurs in the course of the officer's duty, and the officer reasonably believes that it is necessary to monitor or record the conversation or activity for the protection of any person's safety.

Can I install and use tracking devices?

A person must not knowingly install, use or maintain a tracking device, for example in a company car, to determine the geographical location of a person or object. This is so unless the person that is being tracked, or the person in control of the object being tracked, has provided express or implied consent.

Note, on application by a law enforcement officer, a Supreme Court judge or a Magistrate may issue a surveillance device warrant which must be complied with.

Computer (or data) surveillance devices for use other than by law enforcement is not regulated under the Act.

Are there any restrictions on where surveillance devices can be located?

An employer must not knowingly install, use or maintain an optical surveillance or listening device to observe, listen to, record or monitor the activities or conversations of a worker in the toilet, washroom, change room or lactation room in the workplace.

Are there restrictions on the use of material obtained through surveillance?

It is an offence to communicate or publish a record or report of a private conversation or private activity that has been obtained directly or indirectly as a result of using an optical, listening or tracking device.



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

However, there are exceptions to this which include:

- where each party to the conversation or activity have given express or implied consent;
- where communication or publication is in the public interest or for the protection of the lawful interests of the person making it;
- in the course of legal proceedings or disciplinary proceedings.

Breaches of the Act may result in a maximum 2 years imprisonment and/or maximum of 240 penalty units (for natural persons), or a maximum of 1200 penalty units (for corporations).

What does this mean for my workplace?

Employers should exercise considerable caution when installing listening devices in the workplace, as such devices must not be used to inadvertently record private conversations.

Optical surveillance devices may be used to record activities that are not private, such as those occurring outside of a building or in circumstances in which the parties to it ought reasonably to expect that it may be observed by someone else, for example in a shopping centre.

South Australia

The *Surveillance Devices Act 2016* (SA) (**Act**) regulates the installation and use of surveillance devices in South Australia.

Can listening devices be used in the workplace?

A listening device is any device capable of being used to listen to or record a private conversation.

In South Australia, it is an offence to intentionally install or use any listening device to overhear, record, monitor or listen to any private conversation, whether or not the person is a party to the conversation.

This will not apply where:

- the parties to the conversation have given their express or implied consent;
- where the use or installation of the device is reasonably necessary for the protection of the lawful interests of that person; or
- it is in the public interest.

Can optical surveillance devices be used in the workplace?

Optical surveillance devices (for example, CCTV cameras) are commonly used to ensure the safety and security of staff, customers, and property. It is an offence to knowingly install, use or maintain an optical surveillance device to observe or record a private activity without express or implied consent.

Private activities are those which are carried out in circumstances which would indicate the person does not want to be observed by anyone other than a party to that activity, such as bathrooms, change rooms, and shower facilities.

Activities that are carried out in a public place, or which can be readily observed from a public place (for example, in a shopping centre) will not constitute private activities for the purposes of the Act. It is unclear whether office activities are covered by the Act.

Can data surveillance devices be used in the workplace?

Data surveillance devices are devices or programs which can be used to access, track, monitor and record information from a computer. They are commonly used to monitor employees' use of company technology, for example computers and smartphones.

It is an offence to knowingly install, use or maintain a data surveillance device without express or implied consent.

Can tracking devices be used in the workplace?

Tracking devices, such as GPS tracking in work vehicles, cannot be installed, used or maintained for the purposes of determining the location of a person, vehicle or thing without express or implied consent.



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

Are there restrictions on the use of material obtained through surveillance?

It is an offence to knowingly communicate or publish information or material derived from the use of a listening device.

However, this does not prevent the communication or publication of information or material derived from the use of a surveillance device:

- where each party to the conversation or activity has given their express or implied consent;
- the information is communicated to a party to the conversation; or
- it is published or communicated for the purposes of an investigation or relevant legal proceeding.

What does this mean for my workplace?

Bodies corporate which contravene the Act may face a maximum penalty of \$75,000. The maximum penalty is \$15,000 or three years' imprisonment for an individual.

Information which is obtained via a surveillance device, but is in contravention of the Act, may not be relied upon in disciplinary proceedings.

Employers should exercise considerable caution when installing listening devices in the workplace, as such devices must not be used to inadvertently record private conversations.

Optical surveillance devices may be used to record activities that are not private, such as those occurring outside of a building or in circumstances in which the parties to it ought reasonably to expect that it may be observed by someone else, for example in a shopping centre.



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

Western Australia

The *Surveillance Devices Act 1998* (WA) (**Act**) regulates the installation and use of surveillance devices in Western Australia.

Can I install and use a surveillance device in the workplace?

Listening and optical surveillance devices must not be installed or used to record, monitor or listen to a private conversation or activity to which the person is not a party, or to record a private conversation or activity to which that person is a party, without the express or implied consent of each party to the conversation or activity.

A private conversation or private activity is one which is carried on in circumstances that may be reasonably taken to indicate that the parties desire it to be heard or observed only by themselves.

Can I install and use tracking devices?

A person must not knowingly attach, install, use or maintain or cause to be attached, installed, used or maintained, a tracking device, for example in a company car, to determine the geographical location of a person or object. This is so unless the person that is being tracked, or the person in control of the object being tracked, has provided express or implied consent.

Computer (or data) surveillance devices for use other than by law enforcement is not regulated under the Act.

Are there restrictions on the use of material obtained through surveillance?

It is an offence to communicate or publish a record or report of a private conversation or private activity that has been obtained directly or indirectly as a result of using an optical, listening or tracking device.

However, there are exceptions to this which include:

- publication or communication is made to a party in the private conversation or private activity;
- with express or implied consent of each party to the private conversation or activity; and
- in the course of legal proceedings.

Breaches of the Act may result in penalties of up to \$5,000 and 12 months imprisonment for an individual or \$50,000 for a body corporate.

What does this mean for my workplace?

Employers should exercise considerable caution when installing listening devices in the workplace, as such devices must not be used to inadvertently record private conversations. The use of optical surveillance devices (for example, CCTV cameras) may be used to record activities that cannot reasonably be expected to be private.



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

Tasmania

The *Listening Devices Act 1991* (Tas) (**Act**) regulates the installation and use of listening devices in Tasmania.

The Act does not deal with any other forms of surveillance devices, including optical, computer or tracking devices.

Can surveillance devices be used in the workplace?

A person is prevented from using, causing or permitting the use of a listening device to record or listen to a private conversation to which the person is not a party or to record a private conversation to which the person is a party.

A party to a private conversation may record that conversation if:

- all of the principal parties to the conversation consent, expressly or impliedly, to the listening device being used;
- a principal party to the conversation consents to the listening device being used, and:
 - the recording of the conversation is reasonably necessary for the protection of the lawful interests of that principal party; or
 - the recording of the conversation is not made for the purpose of communicating or publishing the conversation, or a report of the conversation, to persons who are not parties to the conversation.

Other exemptions include where:

- a warrant has been granted pursuant to the Act;
- the use of a listening device was granted pursuant to a grant of an authority;
- the use of a listening device to obtain evidence or information in connection a serious offence; or
- hearing of a private telephone conversation is unintentional.

The Act does not deal with the use of optical surveillance or tracking devices.

Are there restrictions on the use of material obtained through surveillance?

It is an offence to communicate or publish a record or report of a private conversation or private activity that has been obtained directly or indirectly as a result of using a listening device.

However, this restriction does not apply where the communication or publication is made:

- to a party to the private conversation;
- with the express or implied consent of all the principal parties to the private conversation;
- in the course of proceedings for offences under the legislation;



National Retail
Association

GUIDE

- where the person making the communication or publication believes on reasonable grounds that it was necessary to make that communication or publication in connection with an imminent threat of serious violence to persons or substantial damage to property, or a serious narcotics offence.

What does this mean for my workplace?

The legislation in Tasmania deals only with the use of listening devices, and prohibits the recording of private conversations in most circumstances.

While the use of optical surveillance devices is not regulated by the Act, if you intend to use surveillance in areas where there may be an expectation of some level of privacy it is recommended that the express consent is obtained from all employees. While not necessarily required by the legislation, it is recommended that written consent is obtained for this purpose.



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

Northern Territory

The *Surveillance Devices Act 2007* (NT) (**Act**) regulates the installation and use of surveillance devices in the Northern Territory.

Can I install and use a surveillance device in the workplace?

A person must not intentionally install, use or maintain any listening or optical surveillance device to listen, monitor or record a private conversation or private activity to which the person is not a party, and without the express or implied consent of each other party to that the conversation or activity.

A private conversation or private activity is a one carried on in circumstances that may reasonably be taken to indicate the parties to the activity desire it to be observed only by themselves, but does not include an activity carried on in circumstances in which the parties to the activity ought reasonably to expect the activity may be overheard or observed by someone else.

Contravention of this requirement means the person may be liable for a maximum of 250 penalty units or 2 years imprisonment.

Can I install and use tracking devices?

A person must not knowingly install, use or maintain a tracking device, for example in a company car, to determine the geographical location of a person or object. This is so unless the person that is being tracked, or the person in control of the object being tracked, has provided express or implied consent.

Contravention of this requirement means the person may be liable for a maximum of 250 penalty units or 2 years imprisonment.

Computer (or data) surveillance devices for use other than by law enforcement is not regulated under the Act.

Are there restrictions on the use of material obtained through surveillance?

It is an offence to communicate or publish a record or report of a private conversation or private activity that has been obtained directly or indirectly as a result of using a listening device, optical surveillance device or tracking device.

However, there are exceptions to this which include:

- where each party to the conversation or activity have given express or implied consent;
- the information is communicated to the other party involved;
- it is published or communicated for the purposes of an investigation or relevant proceeding; or
- it is in the public interest.

What does this mean for my workplace?

Employers should exercise considerable caution when installing listening devices in the workplace, as such devices must not be used to inadvertently record private



National Retail
Association

GUIDE

conversations. The use of optical surveillance devices (for example, CCTV cameras) may be used to record activities that cannot reasonably be expected to be private.

If you intend to use surveillance in areas where there may be an expectation of some level of privacy it is recommended that the express consent is obtained from all employees. While not necessarily required by the legislation, it is recommended that written consent is obtained for this purpose.



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

Australian Capital Territory

The *Workplace Privacy Act 2011* (ACT) (**Act**) regulates the collection and use of workplace surveillance information in the Australian Capital Territory.

What forms of surveillance are regulated?

The Act applies to any business or undertaking, other than where a person engages someone to perform domestic duties.

A worker under the Act includes employees, independent contractors, outworkers, persons doing work experience and volunteers.

A workplace is defined in the Act to include a place where work is, has been, or is to be, carried out by or for someone conducting a business or undertaking.

The Act is specific to workplace surveillance, and it does not deal with the use of listening devices, including whether a camera is used to record sound, which are dealt with separately under the *Listening Devices Act 1992* (ACT).

In general, under the *Listening Devices Act 1992* (ACT) listening devices must not be used to listen to or record a private conversation, unless:

- the use of a listening device under an authority granted by or under a law of the Commonwealth;
- the unintentional hearing of a private conversation by means of a listening device;
- each principal party to the conversation consents to that use of the listening device; or
- a principal party to the conversation consents to the listening device being so used, and:
 - the recording of the conversation is considered by that principal party, on reasonable grounds, to be necessary for the protection of that principal party's lawful interests; or
 - the recording is not made for the purpose of communicating or publishing the conversation, or a report of the conversation, to any person who is not a party to the conversation.

What are the requirements for using workplace surveillance?

Surveillance in the workplace must not commence without at least 14 days prior written notice to workers (a shorter period may be agreed to by the workers).

The notice must state:

- the kind of surveillance device to be used;
- how the surveillance will be conducted;
- who will typically be the subject of the surveillance (departments, groups, employee classifications);



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

- when the surveillance will start;
- whether surveillance will be intermittent or continuous;
- whether the surveillance will be for a stated period or ongoing;
- the purpose for which the employer may use and disclose surveillance records; and
- that the employee may consult with the employer about the conduct of the surveillance.

The notice may be given in the form of a workplace surveillance policy or other suitable document.

During the period of the notice, the employer has an obligation to consult in good faith with its workers about the proposed surveillance. This means the employer must give its workers a genuine opportunity to influence the conduct of the surveillance.

New workers must be given notice of any workplace surveillance prior to commencement of their employment.

Can covert surveillance be used in the workplace?

Covert workplace surveillance means surveillance of a worker in a workplace without prior notification.

Covert surveillance can only be used upon written application to the Magistrates Court in circumstances where a worker is suspected of engaging in unlawful activity at the workplace.

The application must be made in writing and contain the following particulars:

- the grounds the employer has for suspecting unlawful conduct;
- name of the worker;
- actions the employer has already taken to detect the unlawful activity and the result of this;
- description of the premises, place, computer, vehicle or other thing that will regularly or ordinarily be the subject of the covert surveillance;
- the kind of surveillance device that is proposed; and
- details of any prior applications (if applicable).

A covert surveillance authority may be issued for no longer than 30 days.

Is surveillance prohibited in any areas?

The Act prohibits surveillance in non-work areas in a workplace, being:

- a toilet facility;
- a change room;
- a shower or bathing facility;
- a parent or nursing room;



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

- a prayer room;
- a sick bay; or
- a first aid room.

Are there additional requirements for using optical surveillance devices?

Optical surveillance devices must only be used in the workplace if the device is clearly visible and a sign is clearly visible at each entrance to the workplace, advising people that they may be under surveillance in the workplace.

An optical surveillance device includes a camera casing or other equipment.

Are there additional requirements for using data surveillance devices?

Data surveillance devices must only be used in the workplace if the surveillance is conducted in accordance with a surveillance policy. All workers must be notified of the policy before conducting the surveillance in a way that is reasonable to assume that the worker is aware of and understands the policy. The policy must state:

- how the employer's computer resources may, and must not, be used;
- what information about the use of the employer's computer resources (including internet access and electronic communication applications) is logged and who may access the logged information; and
- how the employer may monitor and audit a worker's compliance with the policy.

Are there additional requirements for using tracking devices?

An employer may only conduct surveillance of a worker that involves the tracking of a vehicle using a tracking device if there is a notice clearly visible on the vehicle or other thing stating that it is being tracked.

Can surveillance be conducted on workers outside of work?

The Act prohibits employers from conducting surveillance of a worker whilst the worker is not in the workplace except where the employer conducts surveillance:

- using a data surveillance device and the worker is using equipment or resources provided by the employer; or
- using a tracking device which includes a tracking function that cannot be de-activated.

What are the restrictions on use and disclosure of surveillance material?

Surveillance records can only be used to take adverse action against a worker (e.g. disciplinary action) if the notice provided to the workers stated that surveillance records would be used for such a purpose.

Surveillance records must only otherwise be disclosed if:

- the use or disclosure is for a legitimate purpose related to the employment of a worker or the legitimate business activities or functions of the employer;



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

- disclosure is to a member or officer of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence;
- use or disclosure is for a purpose that is directly or indirectly related to civil or criminal proceedings; or
- use or disclosure is reasonably believed to be necessary to avoid an imminent threat of serious violence to persons or of substantial damage to property.

What are the security obligations of surveillance records?

The Act places an obligation on employers to take reasonable steps to protect surveillance records it holds from misuse, loss, unauthorised access, modification or disclosure.

Employers are required to take steps to destroy or permanently de-identify surveillance records which are no longer needed for any purpose under the Act.

Can a worker request access to surveillance records?

An employer must, on written request of a worker, allow the worker access to surveillance records relating to that worker. If the employer fails to allow the worker access to relevant surveillance records, the records cannot be used by the employer in legal proceedings with the worker or to take adverse action against the worker.

What is the penalty for failure to comply?

An employer commits an offence if they:

- fail to notify employees accordingly of the use of surveillance devices;
- fail to comply with notification requirements for optical surveillance devices;
- fail to comply with notification requirements for data surveillance devices;
- fail to comply with surveillance requirements for the use of tracking devices;
- failure to keep the information secure;
- monitor the conduct of an employee and then use that to take adverse action against the employee;
- conduct covert surveillance without authority;
- uses and discloses information incorrectly; and
- conducts surveillance in a prohibited non-work area (as defined above) or when not at the workplace.

The maximum penalty for these offences ranges from 20 - 50 penalty units for each offence.

What does this mean for my workplace?

The legislation applicable to the Australian Capital Territory provides specific guidance and requirements that employers must follow, especially with respect to covert surveillance.



National Retail
Association

GUIDE

1800 RETAIL
1800 738 245
NRA.NET.AU

Recording Telephone Conversations

In addition to the laws in force in each State and Territory, separate Commonwealth legislation regulates the recording of telephone conversations.

The *Telecommunications (Interception and Access) Act 1979* (Cth) prohibits the recording of a conversation over a telecommunications service without the knowledge of the parties.

For the purposes of the Commonwealth law consent is not required, however the relevant State law may require consent.

For example, a telephone call in Queensland may be recorded without consent provided the parties are aware that the call is being recorded. However, a telephone call in the Australian Capital Territory cannot be recorded if, after being made aware of the intent to record the conversation, the parties do not consent to being recorded.

For more information

Phone: 1800 RETAIL (738 245)

IMPORTANT INFORMATION

The information in this guide is of a general nature. It is not intended to be a comprehensive summary of the law and should not be relied upon as legal advice.

Summary¹

State/Territory	Legislation	Listening Devices	Optical Surveillance Devices	Computer Surveillance Devices	Tracking Devices
Queensland	<i>Invasion of Privacy Act 1971 (Qld) & Criminal Code Act 1899</i>	Must not be used to record, monitor or overhear private conversations, unless by a party to the conversation.	Must not be used to record someone in a place where they would expect to be private (including bathrooms and change rooms).	Not regulated under the Act. ²	Not regulated under the Act.
New South Wales	<i>Workplace Surveillance Act 2005 (NSW) & Surveillance Devices Act 2007 (NSW)</i>	Must not be used to overhear, monitor or record private conversations without express or implied consent.	Must provide written notice before surveillance commences, must be clearly visible, and signs must be displayed at each entrance. Must not be installed in bathrooms or change rooms.	Must provide written notice before surveillance commences, must have a policy in place, and policy must be provided and explained to employees.	Must provide written notice before surveillance commences, and must clearly display notice on vehicle.
Victoria	<i>Surveillance Devices Act 1999 (Vic)</i>	Must not be used to overhear, monitor or record private conversations without express or implied consent.	Must not be used to observe, monitor or record private activities without express or implied consent. Must not be installed in bathrooms or change rooms.	Not regulated under the Act.	Must not be used without express or implied consent.

¹ This summary is not a substitute for the legislation in force in each State and Territory. Please refer to the chapters in this guide for more detailed commentary.

² While certain types of surveillance are not regulated in some States and Territories, it is nonetheless recommended to follow best practice.

South Australia	<i>Surveillance Devices Act 2016 (SA)</i>	Must not be used to overhear, monitor or record private conversations without express or implied consent.	Must not be used to observe, monitor or record private activities without express or implied consent. Must not be installed in bathrooms or change rooms.	Must not be used without express or implied consent.	Must not be used without express or implied consent.
Western Australia	<i>Surveillance Devices Act 1998 (WA)</i>	Must not be used to overhear, monitor or record private conversations without express or implied consent.	Must not be used to observe, monitor or record private activities without express or implied consent.	Not regulated under the Act.	Must not be used without express or implied consent.
Tasmania	<i>Listening Devices Act 1991 (Tas)</i>	Must not be used to overhear, monitor or record private conversations without express or implied consent.	Not regulated under the Act.	Not regulated under the Act.	Not regulated under the Act.
Northern Territory	<i>Surveillance Devices Act 2007 (NT)</i>	Must not be used to overhear, monitor or record private conversations without express or implied consent.	Must not be used to observe, monitor or record private activities without express or implied consent.	Not regulated under the Act.	Must not be used without express or implied consent.
Australian Capital Territory	<i>Workplace Privacy Act 2011 (ACT) & Listening Devices Act 1992 (ACT)</i>	Must not be used to overhear, monitor or record private conversations.	Must provide written notice before surveillance commences, must be clearly visible, and signs must be displayed at each entrance. Must not be installed in bathrooms or change rooms.	Must provide written notice before surveillance commences, must have a policy in place, and policy must be provided and explained to employees.	Must provide written notice before surveillance commences, and must clearly display notice on vehicle.