PiperAlderman

Article Information

Author: Erin McCarthy
Service: Employment & Labour

South Australian Parliament passes the Surveillance Devices Act 2016 (SA)

For many years, the regulation of surveillance devices in South Australia has been less comprehensive than in other Australian jurisdictions.

*For many years, the regulation of surveillance devices in South Australia has been less comprehensive than in other Australian jurisdictions. Recently, the South Australian Parliament took action to bring South Australia in line with other States and Territories by passing the Surveillance Devices Act 2016 (SA) (**the 2016 Act**) and repealing the Listening and Surveillance Devices Act 1972 (SA) (**the 1972 Act**). Ahead of the likely commencement of the new legislation in or early 2017, **Erin McCarthy, Partner** and **Shauna Roeger, Law Graduate** examine the new Act and its impact on how employers can legally conduct workplace surveillance in South Australia.*

Regulation of workplace surveillance in Australia

There are many legitimate reasons why employers may wish to engage in surveillance in the workplace, whether it be to improve security, protect property, ensure the health and safety of staff and customers, and maintain records in case instances of alleged misconduct require investigation. However, along with these considerations is the expectation of employees that they will not be subject to unreasonable invasions of privacy at work and after hours. The surveillance legislation in each of the States and Territories seeks to balance these considerations, but each piece of legislation does so in slightly different ways.

The most stringent regulation exists in NSW and the ACT – where organisations must comply with both the specific workplace surveillance legislation and the general surveillance legislation. The workplace surveillance legislation imposes more onerous obligations on employers, such as providing a written notice of surveillance to employees 14 days in advance of the commencement of surveillance, and consulting with employees about proposed surveillance.

In contrast, in SA, VIC, QLD, WA and NT workplace surveillance is subject to the same restrictions as general surveillance devices. These jurisdictions regulate the use of some or all of the following devices: listening devices, optical surveillance devices, data surveillance devices and tracking devices. There are substantive differences in the legislation across the states in the definitions of the various devices and the extent of the prohibitions and exceptions for their use.

The new SA legislation

Having not been amended for 16 years, the 1972 Act was far less comprehensive than in other States and Territories in that it only regulated the use of listening devices. The 2016 Act seeks to account for more recent technologies in electronic surveillance, bringing South Australia into line with the legislation in most other States and Territories. A “Surveillance device” is defined as a listening device, optical surveillance device, tracking device or data surveillance device, or a device that is a combination of any of those devices. The offences for the unlawful use of each of these types of devices are explained in more detail below.

Listening devices

“Listening devices” are devices that can be used to listen/record a private conversation. Similarly to the 1972 Act, it is an

offence under the 2016 Act to knowingly install, use or cause to be used, or maintain a listening device to overhear, monitor or listen to a private conversation. This applies whether or not the person is a party to the conversation. It is not an offence where all principal parties to the conversation have expressly or impliedly consented.

The main difference under the 2016 Act is that the maximum penalties for the offence have been increased significantly – from $10,000 or 2 years' imprisonment under the 1972 Act, to $75,000 for a body corporate and $15,000 or 3 years' imprisonment for a natural person under the 2016 Act.

Optical surveillance devices

"Optical surveillance devices" are devices that can be used to observe events or record visually, such as CCTV. Common uses of these devices in the workplace include ensuring the security and safety of staff and customers and the protection of property.

Under the 1972 Act visual surveillance devices were regulated only in relation to police warrants. With the result being that there was no restriction on the private use of visual surveillance except to the extent that the visual surveillance device also recorded sound and could also be said to constitute a "listening device". The 2016 Act creates a new offence for knowingly installing, using or maintaining an optical surveillance device to observe or record visually a private activity.

"Private activity" is activity carried on in circumstances that reasonably indicate the person does not want to be observed by anyone other than a party to the activity. Activity carried on in a public place, in premises or a vehicle that can be readily observed from a public place or in circumstances in which the person should reasonably expect to be observed is not private activity for the purposes of the Act.

The exceptions to the definition of "private activity" take many instances of workplace surveillance outside the scope of the prohibition. It is unclear whether an employee working in their office, or a meeting between employees in a private meeting room might constitute "private activity" – this will likely depend on the particular circumstances. However, it is clear that any surveillance occurring in any obviously private areas in a workplace (e.g. bathrooms) would fall foul of the prohibition unless the express or implied consent of those being surveyed has been given. This is slightly less strict than legislation in NSW, ACT and VIC which bans the use of surveillance in private areas of the workplace (eg bathrooms, change room, shower or bathing facilities etc.) regardless of consent.

Data surveillance devices

"Data surveillance devices" are programs/devices that can be used to access, track, monitor or record the input/output of information from a computer. Common uses of data surveillance in a workplace setting would be to monitor employees' use of equipment or resources supplied by the organisation, such as desktop computers, laptops and smartphones.

The 1972 Act was completely silent on data surveillance devices. The 2016 Act makes it an offence to knowingly install, use or maintain a data surveillance device to access, track, monitor or record the input of information into, the output of information from, or information stored in, a computer. Interestingly, there is no definition of "computer" in the Act. However, comparable legislation in other States defines "computer" very broadly (e.g. "any electronic device for storing, processing or transferring information" in NSW and "any electronic device for storing or processing information" in VIC). Based on equivalent legislation in other States we would expect that the term 'computer' would also encompass laptops, tablets and smartphones.

Employers should review their current IT monitoring policies and practices and consider whether employee consent must now be obtained to lawfully continue monitoring. Similarly to the above offences, implied consent is sufficient, however because data monitoring is less visible than other forms of surveillance, care should be taken ensure that employees are fully informed about the types and extent of computer surveillance to which they are subject.

Tracking devices

"Tracking devices" are devices that can determine the geographical location of a person, vehicle or thing. Common uses of tracking devices in a workplace setting include personal GPS tracking devices, GPS devices in work vehicles and devices in smart phones.

Under the 1972 Act tracking devices were regulated only in relation to police warrants. The 2016 Act makes it an offence to knowingly install, use or maintain a tracking device to determine the geographical location of a person, vehicle or thing.

Express or implied consent of the person being tracked, or the person in control of the vehicle or thing, is an exception to the offence.

Employers who use these devices should review and update their policies and ensure that employees being surveyed in this way have given their express or implied consent.

Republication of information

Similarly to the 1972 Act, the 2016 Act regulates the communication and publication of material derived from the use of surveillance devices. This becomes relevant for employers if material derived from surveillance devices reveals employee misconduct and the material is later sought to be used in an internal/external investigation or legal proceedings.

If the employer had the employees' express or implied consent to conduct the surveillance, then there is no prohibition on that material then being communicated or published further. However, if the material is derived from the unlawful use of the device, it is an offence to communicate or publish the information to anyone other than a party to the conversation or activity, unless consent is given by each party. If unlawful surveillance is conducted and that surveillance reveals employee misconduct, then employers may find themselves in a difficult position having not only contravened the law, but then being unable to take disciplinary action against the employee without committing a further offence. This highlights the importance of ensuring any workplace surveillance is conducted strictly within the limits of the Act.

Summary

The introduction of the *Surveillance Devices Act 2016* (SA) represents a substantial increase in the regulation of surveillance devices in SA. Whereas the 1972 Act only regulated listening devices, the new legislation also regulates optical surveillance, data surveillance and tracking devices.

On one view, this is an additional burden for employers with operations in South Australia. However, this legislation does bring South Australia more up to date with developments in other Australian jurisdictions and is to be expected given the progression in surveillance technology over the years. It is vital that employers conduct a careful review of their policies and procedures not only to ensure compliance with the new legislation, but also to ensure that surveillance data (particularly from CCTV, email and internet use, GPS and smartphone data) can be relied upon in disciplinary proceedings if necessary.

Should your organisation require advice on the legality of workplace surveillance or to review your current policies and procedures, please contact a member of Piper Alderman's Employment Relations team.