QUAY INSIGHTS November 2023

The impact of Australia's privacy related laws on employment relationships: Employee surveillance

A. Introduction

A key issue that employers are often interested in, particularly in the current times where more employees are working remotely than ever before, is the steps an employer may lawfully take to survey their employees.

A consideration of this issue requires a close examination of federal as well as state and territory legislation. This article looks at federal and New South Wales laws. The position in other Australian states and territories may differ.

B. An overview of the Privacy Act and TIA Act

The primary federal legislation that is relevant to this question is the Privacy Act 1988 (**Privacy Act**) and the Telecommunications (Interception and Access Act) 1979 (**TIA Act**).

1. Privacy Act

The Privacy Act, incorporating the Australian Privacy Principles (**APPs**), regulates the collection and management of "personal information", which is information or an opinion about an identified individual, or an individual who is reasonably identifiable, and whether or not true or recorded in a material form. Entities regulated under the Privacy Act are Commonwealth Government entities and private sector entities with an annual turnover of more than $3 million. In limited circumstances, other businesses may also be subject to regulation under the Privacy Act.

Employee records exemption

The Privacy Act contains an important employment related exemption for private sector (both for profit and not-for-profit) entities.

This exemption is the "employee records" exemption. Specifically, the Privacy Act does not apply to an act or practice of a private sector entity in relation to an employee record directly related to a current or former employment relationship. An employee record is defined as a record of personal information relating to the employment of the relevant employee and includes, for example, health information and personal information regarding employment-

related matters such as taxation, banking and superannuation affairs, membership of a trade union, and terms and conditions of employment. Any acts or practices of an entity that is or was the employer of an individual are not subject to the Privacy Act if the act or practice is directly related to the existing or former employment relationship and that individual's employment record.

This exemption is limited. It may be the case that it applies only to the use of the employee records, not the original collection of the personal information. This was the approach taken in Jeremy Lee v Superior Wood Pty Ltd [2019] FWCFB 2946. In that case, Mr Lee was dismissed because he would not agree to the collection of a scan of his fingerprint to enable the use of his employer's newly introduced fingerprint scanner to confirm his attendance at his workplace. The Fair Work Commission held that the employee records exception did not apply to exempt the collection of Mr Lee's fingerprint scan from the scope of the Privacy Act as that exception applied only in relation to records that were in existence. This was only a Fair Work Commission decision, and may not be followed in by the Federal Court, given that the exemption is stated to apply to any "act" or "practice", which would seem broad enough to encompass the initial creation of an employee record. Nonetheless this decision demonstrates a narrow interpretation of the employee records exception.

The employee records exemption does not apply to:

- non-employees, such as volunteers or consultants;
- employee records of Commonwealth public sector entities; or
- acts or practices unrelated to the employment relationship.

When might the Privacy Act apply to employee surveillance?

Broadly speaking the Privacy Act applies to the collection, use and disclosure of personal information. Noting the employee records exemption, this means that the Privacy Act is likely to apply to the most common categories of employee surveillance, namely:

- interception and recording of telephone conversations;
- email surveillance;
- closed circuit television (**CCTV**) surveillance;
- device monitoring; and
- finally, the use of biometric data.

Where any of the forms of surveillance set out above occur, personal information of both the employee and, in some cases such as telephone surveillance, individuals with whom the employee interacts, may be collected.

Where the personal information of non-employees may be collected, there would be no scope for the employee records exemption to apply. Therefore, generally speaking, it would be appropriate to assume that the Privacy Act does apply when surveillance of employees is undertaken.

Where the Privacy Act applies (and noting the employee records exemption), then personal information may only be collected where it is reasonably necessary for one or more of the entity's functions or activities and the other requirements of the APPs are satisfied (including, for example, if the personal information collected was sensitive information, such as health information or personal information about an employee's race, sexual orientation, political opinions, union membership, or the like, then the consent of the employee would need to be obtained). This would need to be taken into consideration by an employer where that employer decided to undertake surveillance.

Collection by lawful and fair means

APP 3.5 provides that an APP entity may only collect personal information by lawful and fair means. Therefore, where the Privacy Act does apply, employers would need to give consideration to this in undertaking employee surveillance, including by ensuring that any other applicable legislation is also complied with.

The need for a privacy policy and notice

A regulated entity requires a privacy policy which (amongst other matters) must state how the relevant entity collects and holds personal information and the purposes for which it collects, holds, uses and discloses personal information. If employee surveillance is undertaken, it is very likely to be the case that this would need to be disclosed in the employer's privacy policy, either where the employee records exemption does not apply or because the surveillance may result in the personal information of non-employees being collected.

In addition, APP 5 requires that, at or before the time (or if that is not practicable, as soon as practicable after) a regulated entity collects personal information about an individual, the entity will notify that individual of certain matters. This would include, for example, the purposes for which information is collected and that the privacy policy of the relevant entity contains certain information. Again, this would need to be considered and, where relevant, complied with by employers in undertaking employee surveillance.

Is consent required for collection?

If the Privacy Act applies, consent from the employee would only be required if sensitive information of the employee was collected.

As mentioned previously, sensitive information includes health information or personal information about an employee's race, sexual orientation, political opinions or union membership. If any of these types of information were to be collected through employee surveillance, this would require consent (where the employee records exemption did not apply).

Methods of employee surveillance may include biometric monitoring, which (subject to the employee records exemption) means that employee consent will be required for this, as sensitive information under the Privacy Act also includes:

- biometric information that is to be used for the purposes of automated biometric verification or biometric identification; and
- biometric templates.

Protection and deletion of personal information once collected

If the Privacy Act applies (noting the employee records exemption):

- APP 11.1 requires the employer to protect the personal information held as a result of its surveillance activities; and
- APP 11.2 requires that if an entity holds personal information about an individual and the entity no longer needs the information, the entity must take reasonable steps to destroy or de-identify the information (unless one of a number of limited exceptions applies, for example, the personal information is required to be retained by law).

Employees rights to access personal information

Subject again to the employee records exemption, APP 12 provides that a regulated entity must on request from the relevant individual provide access to that individual to their personal information held by the regulated entity. Where the regulated entity is a private sector entity, that access must be provided within a reasonable period after the request is made unless one of a limited number of exceptions applies, such as that providing access would have an unreasonable impact on the privacy of other individuals. An access charge may be imposed by a regulated private sector entity, provided it is not excessive, and a regulated entity must, if it is reasonable and practicable to do so, provide access in the manner requested by the relevant individual.

Penalties for breach are high

If the Privacy Act does apply to employee surveillance, then the high penalties for breach of the Privacy Act drive home the need for full compliance with that legislation.

In late 2022, the Privacy Act was amended to significantly increase the penalties payable for breach. For corporates, the maximum penalty for serious or repeated interference with the privacy of an individual is the greater of:

- $50 million;
- if this can be determined, three times the value of the benefits obtained from the breach; and
- if the amount referred to in the previous dot point cannot be determined, 30% of the corporate's Australian turnover during the period the breach continued.

As well as being able to commence civil proceedings for certain breaches of the Privacy Act, other enforcement options are available under the Privacy Act, namely enforceable undertakings, infringement notices and injunctions. The Office of the Australian Information Commissioner (**OAIC**) may also issue determinations requiring regulated entities to take particular action in relation to breaches.

Proposed amendment to the Privacy Act

A review of the Privacy Act was commenced by the then Australian Government in late 2019. That review is ongoing. One of the amendments to the Privacy Act which is being considered by the current Australian Government is the removal or dilution of the employee records

exemption. The removal of that exemption would impact on the application of the Privacy Act to employee surveillance in the private sector.

2. TIA Act

Interception generally

The Telecommunications (Interception and Access) Act 1979 (Cth) (**TIA Act**) governs the interception of, and other access to, communications that pass over a telecommunications system. Communication is defined under the TIA Act to apply to telephone calls, SMS, emails and other conversations and messages that may pass over a telecommunications system.

Under the TIA Act, interception of a communication refers to listening to, or recording, a communication passing over a telecommunications system (as it is passing over that system) without the knowledge of the person making the communication.

The TIA Act prohibits the interception of communications unless a specific exemption applies.

Interception of telephone calls

The case of R v Catena [2012] WASC 144 considered the legality of an employer recording telephone calls made by employees during the course of the employer's business (being a stockbroking business). In that case it was noted (at paragraph 59) that:

> *there could be no privacy as between an employee of a broking firm and the firm itself in relation to the content of business telephone communications between staff of the firm and its clients acting in the course of their employment in taking or receiving orders for the purchase of securities or giving advice or information in relation to such actual or potential transactions.*

In other words, for the purposes of the TIA Act, the employer should be taken to be the party to a call relating to its business made by its employee (who would be considered to be the agent of the employer) and therefore no interception would in fact be considered to have occurred vis a vis the employee for the purposes of the TIA Act if the employer recorded, or listened to, such a call as it was passing over a telecommunication system.

Even though, from an employee's perspective, there would be no interception by the employer of employment related calls, this would not apply in the case of the counterparty to any such call. In that regard, the TIA Act does not restrict interception of calls where the person making the communication has knowledge of the interception. Therefore, consent is not required for the interception under the TIA Act made by an employer, but the non-employee party to the call would need to be informed of any interception before it occurred. Best practice would be for this notification to occur at the beginning of the call.

Interception of emails

The TIA Act applies to interceptions by an employer of the emails of its employees as they are sent. If R v Catena applies, or the relevant employee was aware of the interception of his/her email communications, then the prohibition (at least from the perspective of the employee) would not apply. Consideration would however need to be given to the position of persons who sent emails to employees, to determine if interception, within the meaning of the TIA Act, was to occur.

Access to stored communications

The TIA Act also regulates access to stored communications. Access to stored communications is prohibited where this occurs without the knowledge of both the person who sent the communication and the recipient (unless an exemption applies). However, stored communication is defined to mean a communication that, after it has been made, is stored on the equipment of a telecommunications carrier or carriage service provider and which cannot be accessed by a person other than the parties to the communication without the assistance of that carrier or carriage service provider. Therefore, the restrictions imposed on accessing stored communications under the TIA Act would typically not apply to an employer monitoring or accessing any employee's recorded telephone calls.

C. New South Wales legislation

1. Overview

In New South Wales, the Workplace Surveillance Act 2005 (**WS Act**) regulates camera, computer and tracking surveillance of employees (but not listening device surveillance).

For the purposes of the WS Act, "employee" has an expanded definition, including a person employed by a particular employer or its related corporations and can also extend to volunteers and other persons engaged through a labour hire company. The WS Act applies when an employee is at work, that is, when that employee is at a workplace of that employer (or any of its related entities) or when the employee is actually performing work, even if not at such a workplace.

The New South Wales Surveillance Devices Act 2007 (**SD Act**) regulates surveillance generally, including listening device surveillance, and is not limited in its application to employment relationships.

2. WS Act

Types of surveillance

There are three types of surveillance regulated under the WS Act, namely:

- camera surveillance;
- computer surveillance; and
- tracking surveillance.

Camera surveillance is defined in the WS Act to mean surveillance by means of a camera that monitors or records visual images of activities on-premises or any other place.

Computer surveillance is defined in the WS Act to mean surveillance by means of software or other equipment that monitors or records the information input or output (or any other use) of a computer, including the sending and receipt of emails and accessing websites.

Tracking surveillance is defined in the WS Act to mean surveillance by means of an electronic device the primary purpose of which is to monitor or record geographical location or movement, such as a GPS tracking device.

The WS Act generally prohibits an employer from undertaking any of these types of surveillance of an employee while the employee is not at work, except in the case of computer surveillance using equipment or resources provided by (or at the cost of) the employer.

Notice requirements

Except where covert surveillance is permitted, while employee consent is not required, surveillance of an employee by an employer at work is prohibited unless 14 days prior written notice of the surveillance is given (which may occur by email) to the employee (or a shorter period is agreed by the employee). Where surveillance is already in place before an employee is engaged (or will commence earlier than 14 days after the employee is engaged), the employer must give notice to the employee before they start work.

The notice must set out:

- that the relevant type of surveillance is to be carried out;
- how that surveillance will be carried out;
- when the surveillance will commence;
- whether the surveillance will be continuous or intermittent; and
- whether the surveillance will be for a specific limited period or ongoing surveillance.

An exemption is that the employer is not required to provide notice of camera surveillance at a workplace that is not a usual workplace of the employee.

Specific requirements for different types of surveillance

An additional requirement, applicable to camera surveillance only, is that it must not be carried out unless the cameras (or camera equipment) used for the surveillance are clearly visible in the place where the surveillance is taking place and signage stating that surveillance may be undertaken is visible at all entrances to the relevant place.

Computer surveillance must only be carried out in accordance with a policy of the employer and each monitored employee must be notified in advance of the terms of that policy in such a manner that it is reasonable to assume the employee understands the policy. There are no requirements to have a written policy governing CCTV or tracking surveillance however, given the notice requirements of the WS Act, it would be prudent to implement a policy for these types of surveillance.

Where tracking of a vehicle or other device occurs, this must not be carried out by an employer unless a notice is also provided in the vehicle or other device indicating it is subject to tracking surveillance.

Deeming provision: other agreement in place

Surveillance is taken to comply with the notice and other specific requirements outlined above where the relevant employee or a body (such as a trade union) representing a substantial number of employees at the relevant workplace has agreed to that surveillance for a purpose other than surveillance of employees and the surveillance occurs in accordance with that agreement.

Restrictions regarding surveillance

The WS Act:

- prohibits surveillance of employees in any change room, toilet, shower or other bathing facility; and
- provides that (excluding covert surveillance) an employer must not use or disclose any surveillance records except for:
    - use or disclosure for a legitimate purpose related to the employment of employees or the employer's business;
    - disclosure to a relevant law enforcement agency in connection with the occurrence of an offence;
    - use or disclosure in relation to civil or criminal legal proceedings; or
    - use or disclosure if reasonably considered necessary to avert an imminent threat to any person or substantial property damage.

Covert surveillance

Covert surveillance may only be carried out if authorised by a magistrate but only for the purposes of determining whether an employee, or employees, are involved in any unlawful activity at work.

The WS Act expressly provides that covert surveillance must not be carried out for the purposes of monitoring an employee's work performance. Further, as for notified surveillance, covert surveillance must not be carried out in any change room, toilet facility, shower or other bathing facility.

There is a very limited defence to breach of this general prohibition on covert surveillance, which is where the employer proves three matters, namely, that the surveillance was solely for the purposes of ensuring security of the workplace, or persons in it and extrinsic for those purposes; the security of the workplace or such persons would have been jeopardised if the surveillance had not been carried out; and notice in writing was given to the employees (or a body representing a substantial number of them such as a trade union). Generally, any surveillance records made as a consequence of this type of surveillance which is not related to the relevant security matters must not be used in disciplinary or legal proceedings against an employee unless the benefit of doing so outweighs the undesirability of use for this purpose.

The records made as a result of covert surveillance may only be used for limited purposes related to the unlawful activity for which the covert surveillance authority was granted, including for example to assess whether the suspected unlawful activity occurred, in determining what steps should be taken to prevent or minimise the relevant unlawful activity and in disclosure to law enforcement.

An employee is entitled to access covert surveillance records that relate to that employee and any detrimental action the relevant employer proposes to take against that employee (but only if the employer proposes to take such detrimental action). The courts may also make an order that an employee that has been subject to covert surveillance is, on completion of that

covert surveillance, notified of the surveillance and given access to all or part of the surveillance records.

Breaches

Breaches of the WS Act may attract maximum penalties in the order of $2,200 to $5,500.

Relevant cases

In *Krav Maga Defence Institute Pty Ltd t/a KMDI v Markovitch* [2019] FWCFB 4258: the employer used cameras at its martial arts gym to observe its employee Mr Markovitch. Mr Markovitch was summarily dismissed because CCTV footage showed him using his phone on numerous occasions when he was expected to be supervising his classes. Mr Markovitch was aware of the cameras, however, the employer had not provided 14 days' notice of the camera surveillance as required by section 10 of the WS Act and there were no signs advising of the surveillance as required by section 11 of the WS Act.

The Full Bench of the Fair Work Commission accepted there was sufficient evidence to support the employer's submission that the surveillance had occurred with the agreement of the employee. It was held that the agreement did not need to be in writing and could be implied. In this case, it was implied as, for example, Mr Markovitch had authorised the payment of the costs for the installation of the cameras.

Importantly, the Full Bench determined that, even if the CCTV footage was obtained improperly, it was still capable of being admitted as evidence. In this regard, the Full Bench took into consideration section 138(3) of the Evidence Act 1995 (Cth) (No. 2, 1995) (as amended), even though it was not bound by that section. The section sets out the matters that need to be taken into consideration in deciding whether a court should admit illegally obtained evidence.

In the case of *Secure Logic Pty Ltd v Noble (No. 3) [2021] NSWSC 675,* Secure Logic, the employer of Mr Noble, directed another employee (without Mr Noble's knowledge) to take documents from Mr Noble's work laptop, install a key-logging program onto his work laptop and both access his private website and cause emails from his private account to be automatically forwarded to a Secure Logic email account.

The NSW Supreme Court determined that "computer surveillance", within the meaning of the WS Act, refers to continuous monitoring or recording of the employee using computer software to track computer usage. The Supreme Court considered that periodically downloading files from an employee's work computer without their knowledge or consent was not covert computer surveillance, as the continuity element was absent. On the other hand, the installation of key-logging software on Mr Noble's laptop (again, without prior notification) was covert computer surveillance because it did meet this continuity requirement. That conduct was found to contravene the WS Act. Finally, accessing Mr Noble's private website and private emails did not contravene the WS Act because it did not occur while Mr Noble was at work and the Court considered it unlikely that this conduct involved the use of a work surveillance device, within the terms of the WS Act.

3. SD Act

Where the SD Act applies, it will be necessary for an employer to comply both with any relevant requirements of the WS Act (noting the WS Act does not apply to recording conversations) and the SD Act.

Recording private conversations

The SD Act prohibits the use of listening devices to record private conversations (irrespective of whether the person making the recording is or is not a party to the conversation) except in particular circumstances. It applies more broadly than telephone conversations. A private conversation is defined as a conversation where the circumstances indicate that at least one of the parties intends that the conversation will be listened to only by the direct parties to the conversation, or by those direct parties and another person who has the consent of all of those parties to do so. A private conversation does not include a conversation made in any circumstances in which the parties to it ought to reasonably expect that it might be overheard by someone else.

There is also an exemption from the general prohibition where the person recording the private conversation is a party to that conversation, and all principal parties consent. An employee's consent would be required in such instances. Consent should be sought as part of the employment contract (or, if a telephone surveillance policy was put in place at a later time, then prior to the surveillance commencing). Similarly, consent would be required to be obtained from a non-employee party to the call under the SD Act and, again, this should be sought at the commencement of the call.

Relevant decisions regarding recording conversations

The two cases considered below demonstrate that different approaches have been taken by the Fair Work Commission as to whether to allow recordings of conversations that may have occurred in circumstances that breached the requirements of the SD Act.

In the Fair Work Commission decision, *Re Kelly Walker (No 2)* [2019] FWC 4862 the question of whether to admit a secretly obtained recording of a meeting with management into evidence was considered. The Deputy President assessed the applicant's argument that the evidence was not illegally obtained because of the exemption under the SD Act "where the recording of the conversation is reasonably necessary for the protection of her lawful interests".

Having considered the case law, it was noted that the power to admit evidence, illegally obtained or otherwise, is found in section 590 of the Fair Work Act 2009 (Cth) which allows the Commission to inform itself in such a manner as it considers appropriate. The Commission's decision to admit evidence is an exercise of discretion. It was noted that each case will turn on its own facts. The Commission did not have jurisdiction to determine whether a secret recording was obtained unlawfully under the SD Act or whether there has or have been breaches of the WS Act. Nonetheless, the application to admit the evidence in this matter was ultimately dismissed.

In a second Fair Work Commission decision, *Harrison v Trustee for the Trimatic Management Services Unit Trust (T/A TSA Group)* [2020] FWC 2486, the applicant sought to use an audio recording of a meeting between the applicant and her manager in an unfair dismissal case. It was noted in the decision that the SD Act is based on the principle that, with a few limited

exceptions, private conversations should not be recorded by one party without the consent of the other party. The applicant did not have consent of her manager to record the meeting and it was revealed in the recording that the manager had expressly stated that it was not permissible to record the meeting. It was determined that the recording of the meeting was contrary to the SD Act and unlawful, however, being a Commission and not being a court bound by the rules of evidence, the recording was permitted to be included as part of the evidence.

Optical surveillance devices

The SD Act regulates the use of optical surveillance devices (devices used to record visually or observe activity), including of course CCTV. An optical surveillance device must not be used in premises or a vehicle if installation, use, or maintenance of the device involves entry into the relevant premises or vehicle, or interference with the vehicle, without the consent of the owner or occupier (consent from the possessor or owner of an object would also be required if such activities involved interference with that object). Therefore, the SD Act would not restrict the ability of an employer to undertake CCTV surveillance in its own premises (or in other premises, if consent is obtained from the owner or occupier).

Relevant decision regarding optical surveillance

In *Mulhearn v Merit Homes Pty Ltd [2015] NSWCATCD 139* the applicants sought to tender to the New South Wales Civil and Administrative Tribunal photographs of images obtained from a time lapse surveillance camera installed by the applicants on a building adjoining the site where building works were carried out by the respondent. The respondent argued that the surveillance camera footage was taken in breach of the SD Act and therefore should not be admitted. Given the camera was installed with the consent of the owner of the adjacent building, there was no breach of the SD Act. The Tribunal also found that, notwithstanding the wide definition of employee in the WS Act, the respondent was not the employee of the applicant (the respondent was a building contractor of the applicants). Therefore, the WS Act did not have any application.

Data surveillance devices

The SD Act regulates the use of data surveillance devices, including any device or program that may be used to record the input/output of information in a computer. A data surveillance device may be used, unless the installation, use or maintenance of the device involves entry to premises without the consent of the owner or occupier of the premises, or interference with a computer or computer network without the consent of the person having possession or control of the computer or computer network. Consent from the employee is only required if the surveillance involves entry to the employee's premises or interference with a computer or computer network in the possession or control of the employee.

Device monitoring

The SD Act regulates the use of tracking devices, which include any electronic device capable of being used to determine or monitor the geographical location of a person or object. Use of a tracking device to track a person will be permitted if the consent of that person is obtained, and use of a tracking device to track an object will be permitted if the consent of the person

possessing or controlling that device is obtained. Consent should be obtained in writing at the commencement of the employment relationship or, if later, before tracking commences.

D. Other Australian States and Territories

This guidance note contains guidance only on Australian federal law and the laws of New South Wales. There is other legislation and case law that will be relevant in other Australian states and territories, and the application of that law will depend on whether an employment relationship has a relevant jurisdictional nexus.

Each state and territory has legislation that generally regulates surveillance activities. But only New South Wales, the Australian Capital Territory, and (to a certain extent) Victoria have surveillance legislation that deals specifically with surveillance by employers of employees. This legislation governs the same type of surveillance as is governed under the WS Act and the Victorian legislation contains a general prohibition on the use by an employer of optical or audio surveillance in workplace toilets, washrooms, change rooms, or lactation rooms. Although there is different legislation throughout Australia, typically consent is required for lawful surveillance by employers of employees and therefore it would be appropriate for an employer in Australia to require employees to consent to a documented surveillance policy.

Contacts

Angela Flannery
Partner

Quay Law Partners
Level 32, 180 George Street,
Sydney NSW 2000
T +61 419 489 093
E angela@quaylaw.com
www.quaylaw.com

Dave Poddar
Partner

Quay Law Partners
Level 32, 180 George Street,
Sydney NSW 2000
T +61 422 800 415
E dave@quaylaw.com
www.quaylaw.com