



# Australia: Relevant legislation

We have identified the following key pieces of legislation which are applicable to employee IT monitoring in Australia. Note that there is other legislation which is applicable which we have not included in this document.

Also note that legislation in Australia may differ according to the state. Where we discuss specific state legislation, we have specified the state.

## **Workplace Surveillance Act 2005 (New South Wales or NSW) and Workplace Privacy Act 2011 (Australian Capital Territory or ACT):**


- Regulate camera, computer and tracking surveillance;
- Employers may conduct types of surveillance in respect of employees/workers when:
  - The employee is at work/'in a workplace'; and
  - Employees are notified in writing of the surveillance. There are detailed notification requirements.
- Computer surveillance must be conducted in accordance with a policy, and employees should be aware of and understand the policy;
- Neither of the Acts expressly state that accessing/reviewing an employee's mobile telephone records is surveillance. However it could constitute 'computer' surveillance. Monitoring an employee's calls over a VOIP network could constitute computer surveillance under both Acts.

## **Privacy Act 1988:**

This Act regulates how "personal information" should be handled.

- Provides for the Australian Privacy Principles (APP):
  - Openness and transparency (including having a privacy policy);
  - Option of anonymity for individuals;
  - Only collect personal information that is necessary for the entity's function(s);
  - Notice must be given about the collection of personal information;
  - Outline how personal information is to be used and disclosed;
  - Adhere to requirements relating to cross-border disclosure of personal information;
  - Ensuring personal data collected is accurate, up to date and complete, as well as relevant to any purpose for which it is used or disclosed;
  - Personal data is kept secure;
  - Rights of access and rectification for individuals over their personal information;



- 
- Notification in the event of breaches to either or both of the affected individual(s) and the Office of the Australian Information Commissioner;
  - Exemption for 'employee records' (defined under case law below), but only for private sector.

### **Telecommunications (Interception and Access) Act 1979:**

- It is an offence to intercept a communication passing over a telecommunication system.
- There are only limited exceptions to this prohibition, such as if a warrant has been issued.

### **Evidence Act 1995**

- Evidence is not to be admitted if it has been obtained:
  - Improperly or in contravention of an Australian law; or
  - As a consequence of an impropriety or contravention of an Australian law.
- The evidence can, however, be admitted if the desirability of admitting the evidence outweighs the undesirability of admitting it.

# Principles deduced from case law

The cases that were reviewed in Australia rarely involve insider threat activity, such as industrial espionage or intention by employees to defraud or exploit confidential information. There remains a disconnect with the number of reported employment law cases which deal specifically with insider threat monitoring, where rogue insiders have been dismissed by their employers and have challenged their dismissal leading to an examination by the courts of the monitoring techniques deployed. The vast majority of reported cases relate by way of subject-matter to situations of video surveillance, of social media misuse or, for example, excessive personal use of company IT systems by employees.

In Australia employees may have limited expectations around their privacy rights because of the breadth of the “employee records” exemption. This in turn may explain why there have been so few cases in this area.

The ‘employee records’ exemption means that the handling of personal information by a private sector employer is exempt from the Privacy Act if it is directly related to:

- The employee’s current or former employment relationship;
- An employee record related to the employee – this is defined as a record of personal information about the employee. E.g. health information, terms and conditions of employment, emergency contact details, sick leave details, taxation, performance information.

This does not exempt the organisation from obligation towards individuals before they become an employee (e.g. job applicants, potential candidates). A policy on monitoring must be in place, and consistently and fairly applied by the employer.

## Social media

There are a greater number of cases related to employees’ use of social media. If a social media post adversely affects the employer’s business, it may be sufficient to warrant dismissal (whether on private or corporate system).

Examples of considerations for fair/unfair dismissal cases in relation to social media posts:

- Serious damage caused to the relationship between employee and employer;
- Damage caused to employer’s interests;
- Potential damage caused to relationship between employee and other employees;
- Behaviour incompatible with employee’s duty as an employee;
- Behaviour inconsistent with the employer’s policy/code of conduct;
- Behaviour constituted serious misconduct;
- Behaviour had occurred before (employee had a history of misconduct).

But, employer must have a social media policy, employee awareness and training on social media use.

## Illegally gathered evidence

Courts and tribunals are prepared to exclude evidence gathered in breach of a law or as a result of surveillance that is deemed an invasion of an employee’s privacy.



# The future

Trends that can be identified:

- The ability to have evidence excluded because surveillance is found to be an invasion of an employee's privacy may increase the number of cases which challenge employee monitoring before the courts.
- Employees may become more aware of the limits to the "employee records" exemption in respect of the Privacy Act. Employees may become more aware of the limits of the employee records exemption from the
- GDPR: Australia is not currently recognised as providing adequate protection of personal data as defined by GDPR. This means that additional safeguards may need to be in place in order for organisations to transmit personal data from Australia to the EU. Australian companies that collect personal data from EU citizens and companies with established operations in the EU should consider whether their operations fall within the scope of the GDPR and, if so, the steps that need to be taken to achieve compliance with its requirements.

Organisations must be aware that legal considerations for employee monitoring will vary from organisation to organisation and specific issues will arise depending on the nature of the organisation undertaking monitoring and the risks it is trying to mitigate. Dentons UK and Middle East LLP (Dentons) prepared a report for NPSA on Employee IT Monitoring in March 2018 (the Report), to serve as a legal resource only, it is not a substitute for professional advice. This document provides a snapshot of some of the information contained in the Report and must not be read in isolation. Neither the Report nor this document are designed to provide legal or other advice and you should not take, or refrain from taking, action based on their content. The Report and this document are not a comprehensive report of all the information or materials that are relevant to this area of law, and do not address any particular concerns, interests, value drivers or specific issues you may have. This is a complex area of law that is changing rapidly. If you require assistance with a specific issue, you should seek legal advice from an appropriately qualified professional.

Organisations planning to implement or review existing employee monitoring should seek their own professional advice.

The Report (and therefore the information contained in this document) was current as of the date of the Report publication (being March 2018). Dentons owes no duty to you to update the content of the Report or this document at any time for any reason. Please note the Report and this document do not represent the views of NPSA or Dentons. Neither NPSA nor Dentons UK and Middle East LLP accept any responsibility for any loss which may arise from reliance on the Report and/or this document.