

--- Excerpt from "INTRODUCTION" ---

**What the Act does not regulate**

[18] Whilst the Workplace Surveillance Act regulates how covert surveillance may be conducted, it largely leaves overt surveillance unregulated. As such, provided an employer complies with the notification requirements under the Act, it is largely free to conduct overt surveillance in any manner that it chooses without any need to justify the need for, or reasonableness of, the surveillance.

[19] The Act does not require employers to obtain employees' consent at any stage to conduct surveillance. Employers will be entitled to conduct surveillance where either notification requirements are met or a covert surveillance authority is obtained. Employers may, however, need to seek consent to reduce the default notice period of 14 days – see [210].

[20] The Act does not regulate the interception of telecommunications.....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

**Interaction with other legislation**

*Occupational Health & Safety Act*

[30] Section 8 of the Workplace Surveillance Act provides that the operation of the Act is not limited or otherwise affected by a requirement imposed under the *Occupational Health and Safety Act 2000* (NSW). As such, it will not be a defence for an employer that breaches the Workplace Surveillance Act to claim, for example, that covert surveillance was conducted in order to comply with occupational health and safety requirements.

[31] If an employer believes it needs to conduct urgent covert surveillance for occupational health and safety reasons, it should use the occupational health and safety consultation regime under Part 2, Division 2 of the *Occupational Health and Safety Act 2000* (NSW) to get agreement for any such surveillance. Any such agreement will generally enable.....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

*Private inquiry agents & security industry Acts*

[41] The requirements of the *Commercial Agents and Private Inquiry Agents Act 1963*, *Commercial Agents and Private Inquiry Agents Act 2004* and the *Security Industry Act 1997* are not affected by the Workplace Surveillance Act. Appropriate licences still need to be obtained in relation to relevant activities covered by those Acts. A covert surveillance authority issued under the Workplace Surveillance Act will not exempt.....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

## --- Excerpt from "NOTIFIED SURVEILLANCE" ---

*Agreement regarding non-employee surveillance*

[185] Surveillance is deemed to comply with notification requirements (ie. notice is not required to be provided) if (s.14):

- the employee, or a body representing a substantial number of employees at the workplace, has agreed to the carrying out of surveillance at the premises or place where the surveillance is taking place for a purpose other than surveillance of employees; and
- the surveillance is carried out in accordance with that agreement.

[186] Importantly, these provisions effectively enable hidden surveillance to be conducted without a covert surveillance authority, provided the purpose of the surveillance is not to monitor employees.

[187] For example, employees may agree pursuant to an industrial agreement that an entrance to their workplace that is primarily used by clients is to be kept under hidden camera surveillance for the purpose of monitoring clients who enter the premises. As part of the agreement, the employees may agree that notices are not required to be erected indicating that that area is kept under hidden surveillance or that employees are to be otherwise notified of the presence of cameras. In such a case, despite the fact that employees are not being notified of the surveillance, the employer would generally be deemed to have complied with the notification requirements under the Act.

[188] From employees' perspective, it is desirable to ensure that any such agreement specifically addresses each notification requirement that would otherwise apply under the Act, and specify whether or not it has to be met under the agreement. This is because, if the agreement remains silent in relation to any particular such requirement, the employer will not be required to comply with.....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

--- Excerpt from "NOTIFICATION  
REQUIREMENTS" ---

**[198] Notification requirements**

***Notice period***

[208] An employer must provide written notice at least 14 days prior to commencing surveillance (s.10(2)). However, an employee may agree to a shorter period (s.10(2)). Written notice can include notice provided via email (s.10(5)).

[209] The Act does not place any limitation on the manner in which notification may be provided, other than that it be in writing. As such, whilst notification via email will, in many cases, be the most efficient method of notification, other means of communication, such as staff memos, may be used.

[210] If an employer envisages that it may need to conduct surveillance at short notice in the future, it should seek consent from employees to provide the required shorter notice period before such need arises, eg. a retailer may commonly need to set up and commence surveillance on 24 hours' notice when it learns that stock is being stolen in order to immediately deter further thefts. In this case, the retailer should seek consent from employees to provide 24 hours' notice before.....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

[223]

**Sample Surveillance Notice**

(via email)

**SURVEILLANCE NOTICE**

*Pursuant to the Workplace Surveillance Act 2005 (NSW), management wishes to notify all workers of surveillance that is conducted of employees whilst at work.*

Action required

\* read this notice carefully; and

\* acknowledge receipt by reply email with "received" in the body of the email.

**Camera Surveillance**

*Permanent camera surveillance of all shop floor and cash handling areas will commence on 1 June 2006. Cameras will be placed through-out stores in appropriate locations. All cameras will be clearly visible and notices will be displayed near all entrances to affected areas. Surveillance images will be monitored by security staff and will be accessible by all managers. All surveillance will be conducted in accordance with our CCTV Surveillance Policy. Cameras will operate 24 hours, 7 days per week.*

**Computer Surveillance**

*Permanent computer surveillance of emails will commence on 1 June 2006. Logs and records will be made of all incoming and outgoing emails that are received or sent through our.....*

[SAMPLE ONLY - REMAINDER OF NOTICE NOT INCLUDED HERE]

-- Excerpt from "COMPUTER SURVEILLANCE" --

**Computer surveillance**

[268] Computer surveillance of an employee can only be carried out if (s.12):

- it is in accordance with a policy of the employer on computer surveillance of employees at work; and
- the employee has been notified in advance of that policy in a way that it is reasonable to assume that the employee is aware of and understands the policy;

[269] The Legislative Assembly Second Reading Speech indicates that the notification requirements are not intended to be onerous and do not, for example, require notices on computers or a notice each time an employee logs on to a computer<sup>1</sup>. Employees only need to be made aware of the employer's policy, ie. employees do not need to be notified upon each individual instance of computer surveillance. For example, a large employer may include notices in induction and training courses and email regular reminders whereas a small business may discuss the policy with each employee and place the policy on a work noticeboard.

*Drafting & amending computer surveillance policies*

[279] An employer will only be entitled to monitor use of its computers in accordance with the terms of a policy that it has in place regarding computer surveillance. As such, an employer will need to ensure that the policy covers all circumstances in which it will seek to carry out computer surveillance.

[280] Employers should consider drafting provisions broadly (eg. computer surveillance may be conducted wherever the employer considers it necessary for the purposes of its business) whilst at the same time, without limiting the generality of the broad provisions, include specific circumstances in which surveillance may.....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

[291]

**Sample Computer Surveillance Policy Terms**

**COMPUTER USAGE POLICY**

**SURVEILLANCE & MONITORING**

*The use of computers, email, the internet and the I.T. network is monitored for I.T., security, performance assessment and risk management purposes. Such use may be monitored in any of the following ways.*

a) **Email:** *Logs are kept to monitor all incoming and outgoing emails received or sent through the I.T. network. Logs record sender and recipient details, dates, times, subject and message content. Emails may be read by I.T. staff or scanned by filtering software in accordance with our Email Policy.*

b) **Internet:** *Logs are kept to monitor internet usage. Logs record internet websites visited, originating computers, times, pages viewed and page download sizes. The logs are monitored by I.T. staff to ensure compliance with our Internet Usage Policy.*

c) **File server:** *Logs are used to monitor files that are accessed from and placed on file servers. Logs record.....*

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

--- Excerpt Only ---

**Prohibited Types of Surveillance**

**[355] Change rooms & bathrooms**

[356] An employer cannot carry out surveillance of employees in any change room, toilet facility or shower or other bathing facility at a workplace (s.15).

***Impact on camera surveillance***

[366] The impact of this prohibition on camera surveillance is clear. Employers must ensure that cameras are not positioned such that they can view employees in workplace change rooms, toilet facilities or bathing facilities.

***Impact on computer & tracking surveillance***

[376] A less obvious impact of the prohibition is that, as surveillance is defined to include computer and tracking surveillance (see [62]), it appears that employers must consider the need to either ban employees taking any item that can be placed under computer or tracking surveillance into workplace change rooms, toilet facilities or bathing facilities or ensure that such items cannot be tracked in such areas. Common items of this nature include, for example, laptops and uniforms containing RFID tags. These steps appear necessary not only to prevent a breach of the Act by the employer, but also, and equally importantly, to prevent the existence of safe-havens, eg. to prevent employees from taking laptops into these areas and using them knowing that they cannot be placed under surveillance whilst in those areas.

[377] To address this issue, employers may consider placing notices outside relevant areas prohibiting employees taking tracked items in with them. Alternatively, it may be possible to de-activate computer or tracking surveillance devices at entrances.....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

--- Excerpt Only ---

**[425] Blocking emails or internet access**

***Policies cannot prevent communication with industrial organisations***

[496] An employer's policy on email and internet access cannot provide for preventing delivery of an email or access to a website merely because (s.17(4)):

- the email was sent by or on behalf of an industrial organisation of employees or an officer of such an organisation; or
- the website or email contains information relating to industrial matters (within the meaning of the *Industrial Relations Act 1996* (NSW)).

[497] The purpose of this prohibition is generally to ensure that employers do not unduly prevent employees from informing themselves of, and being informed of, their rights as employees and communicating with industrial organisations.

[498] However, the Act does not place a blanket prohibition on employers blocking emails from, or access to websites of, employee industrial organisations. This is by virtue of the use of the words "merely because" which indicates that such blocking will be permitted where other reasons for the blocking exist.

[499] The Legislative Council Second Reading Speech provides the following examples demonstrating when blocking will be permitted<sup>2</sup>:

- If an employer has a policy of not allowing access to any external website on its computers, there will be no compulsion to provide access to websites containing information relating to industrial matters. This is because internet access to the website containing industrial matters is being prevented on the basis that all access to external websites is blocked.
- If an employer operates a "white list" (ie. a list of websites to which access is provided), the employer will not be forced to add websites containing industrial matters to.....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

--- Excerpt from "COMPLIANCE CHECKLIST" ---

### **STEP-BY-STEP COMPLIANCE GUIDE & CHECKLIST**

[208-801] A suggested checklist is set out below for employers seeking to ensure compliance with the Act. The checklist aims to provide a detailed guide for employers from the beginning to the end of the compliance process and should enable identification of all compliance measures that need to be taken, and the manner in which all surveillance related policies and procedures need to be amended, based on the employer's current and proposed surveillance practices.

[208-802] It is intended that the checklist will be used in conjunction with the main body of the text. Cross-references have been included through-out the checklist to areas of the text containing relevant detailed information and.....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

#### **[208-830]**

#### **Notified (ie. Overt) Surveillance**

##### **Identify employees to be notified**

- identify all potential types of current and new employees that fall within meaning of "employee" (see [208-73]) who are required to be notified under s.10 (see [208-151])
  - remember:
    - employers that are members of corporate groups must treat employees of related corporations as their own employees (see [208-96] & [208-117])
    - employee working a place that is not their usual workplace not required to be given notice regarding camera surveillance (see [208-173])

##### **Assess need for agreement for non-employee surveillance**

- consider whether employer wishes to enter into agreement with employees regarding conducting surveillance for purpose other than surveillance of employees, eg. monitoring stock or occupational health and safety reasons, which will permit employer to avoid notification requirements (see [208-185])
  - if so, negotiate appropriate agreement with employees
  - if such agreement concluded, no further steps required to comply with notification requirements regarding surveillance with which agreement concerned provided agreement complied with

### **Assess need for notice period less than 14 days**

- review whether employer may need to commence camera, computer or tracking surveillance with less than 14 days' notice which is default notice period required (see [208-208]).
  - if yes, seek consent from employees to provide an appropriately shorter period of notice (see [208-210]).....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

### **Preventing prohibited types of surveillance**

#### **Change rooms, toilets & bathing facilities**

- ensure policies and procedures prohibit camera, computer and tracking surveillance of employees whilst in workplace change rooms, toilet facilities or showers or other bathing facilities (see [208-356] - [208-376])
  - in particular, identify all items that could be placed under computer or tracking surveillance and which could be taken by employees into workplace change rooms, toilet facilities or showers or other bathing facilities (eg. laptops and clothing containing RFID tags) (see [208-376])
    - ensure employees prohibited from taking such items into such areas, that tracking devices de-activated at entrances and/or tracking cannot occur in such areas.....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

#### **Employee not at work**

- identify all circumstances in which, and items in relation to which, employees could be placed under camera, computer or tracking surveillance whilst not at work using a "work surveillance device" (see [208-389])
  - remember, prohibition does not appear to apply to non-work surveillance conducted using something other than a "work surveillance device" (see [208-401])
- identify all types of non-work computer surveillance to which prohibition does not apply by virtue of exemption regarding use of employer's computer equipment or resources (see [208-414])
- ensure policies and procedures prohibit and prevent conduct of non-work surveillance using a "work surveillance device" unless permitted under exemption regarding use of employer's computer equipment or resources (see [208-389]).....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

Blocking emails & websites

- review whether employer needs to (see [208-440]):
  - block any emails sent to or by employees; or
  - block access to websites
- if so, ensure policy on email and internet usage is in place (see [208-426] & [208-440]) and that policy:
  - specifies that employer:
    - may block emails sent to or by employees and reasons for which this may occur;
    - may block access to certain internet sites and reasons for which this may occur.
  - is written in plain language to assist employer in meeting requirement that it is reasonable to assume that employees have understood policy (see [208-442])
  - does not cause blocking in breach of the prohibition relating to the blocking of communications from, and information provided by, industrial organisations (see [208-496]).....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

--- Excerpt from FAQs ---

**FREQUENTLY ASKED QUESTIONS**

**Can video surveillance, including hidden surveillance, be set-up to monitor customers or other non-employees?**

[861] The Act does not regulate surveillance of persons who are not employees. As such, surveillance of any areas (regardless of whether the surveillance is overt or covert) in which employees will not be captured within view of cameras is not covered by the Act.

In most cases, however, it is unlikely that there will be areas of a workplace in which employees will not be seen (ie. kept under surveillance). If an employee will be captured in surveillance images, the surveillance must comply with the Act. The fact that the primary purpose of the surveillance is to monitor non-employees does not exempt it from the Act.

If an employer wishes to set up hidden surveillance for a purpose other than monitoring employees (eg. to monitor certain stock in shops that is regularly being stolen).....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

**Does the Act prevent an employer from reading employees' emails?**

[862] No. The Act does not prevent employers from reading employees' emails, provided applicable notification requirements have been met (see generally [140] and, in particular, [268]). This is despite the fact that the Act prohibits employers from.....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

**Does the Act prevent an employer from monitoring websites visited by employees?**

[863] No. The Act does not prevent employers from monitoring websites that employees visit, provided applicable.....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

**Can employers monitor employee use of email, computers and the internet?**

[864] Yes, employers can monitor employee use of email, computers and the internet provided the employer has .....

[SAMPLE ONLY - REMAINDER OF TEXT NOT INCLUDED HERE]

## Other FAQs Include:

**Can employers screen and block emails and websites, eg. for I.T. security and liability risk purposes?**

**Can an employer place an employee under secret surveillance for the purpose of investigating sick leave and workers compensation claims?**

**Is it permissible for an email and internet policy to provide for the blocking of emails from, or access to websites of, industrial organisations under any circumstances?**

**Is consent from employees required for any form of surveillance?**

**Does the Act apply to home offices or others working from home?**

**Does the Act apply in relation to surveillance of family members in family businesses?**

**Is an employer required to comply with notification requirements if surveillance is being conducted for occupational health and safety purposes?**

**Does the Act override obligations under the Occupational Health & Safety Act?**

**Does the Act regulate the manner in which non-hidden (ie. overt) camera surveillance may be conducted?**

**Can non-hidden (ie. overt) camera surveillance be set-up to monitor employee performance?**

**Does use of objects such as mobile phone and credit card records that may incidentally show an employee's location constitute tracking surveillance?**

**Can members of corporate groups conduct surveillance of each others' employees to avoid the notification provisions of the Act?**

**Can an employee have more than one employer?**

**Is a voluntary worker an employee?**

**Is an employee considered to be at work even if they are not working, eg. using their computer during a lunch break or attending their workplace (such as a gym) in their personal time?**