Workplace Surveillance

Considerations for Queensland
Agenda

• Electronic Surveillance in the Workplace – Current Environment
• NSW Workplace Surveillance Act – Overview and Objectives
• Monitoring Information Assets – Risks and Issues
• Monitoring and Surveillance – Policy Requirements
Electronic Surveillance in the workplace

The current market environment
Current Framework

- State based legislation regulating video surveillance and telecommunication interception.
- Federal Privacy Act and Privacy Act (Private Sector) amendments.
- Federal Privacy Principles

**NSW Workplace Surveillance Act**

The most applicable piece of legislation that provides guidance to employers with respect to how and what they can undertake electronic surveillance in the workplace.
Current Events

• QLD, VIC, ACT and WA reviewing requirements for electronic monitoring looking predominantly at the NSW Workplace Surveillance

• Australian Workers Union (Australia’s Largest Union) largely endorsing the NSW workplace Surveillance Act and providing discussions and recommendations around the protection of personal privacy.

• Workchoices – significant changes to an employees ability to make and follow through with an unfair dismissal claim.

• Convergence of technology and business processes making surveillance and more monitoring easier.
Why look at the NSW Workplace Surveillance Act?

It is inevitable that part, or all of the NSW Workplace Surveillance Act will be incorporated in Federal Industrial Relations Reforms and state based legislation.

Aside from proactively preparing for the likely inclusion of more uniform federal requirements for workplace surveillance managers must consider the legal and employee risks associated with monitoring and surveillance activities that are too light, too heavy or not appropriately communicated.

Implementing the provisions of the workplace surveillance act are effective risk management strategies.
The Privacy Debate

The main argument against electronic surveillance is largely related to Privacy.

Despite the fact that they are using government or corporate equipment and networks staff may consider that their e-mails and web browsing among other electronic activities are private.

In some cases access controls and security features of a network (passwords etc) give the user an illusion of privacy and they may not be aware that their browsing activities and e-mail content can be scrutinised. It may not be understood that the purpose of access controls is to prevent unauthorised access.
The Privacy Debate

It is apparent that there is a general expectation, by staff, that law exists which protects their privacy in the workplace, while this is true to a certain extent, it is less so than most employers and employees realise”

The facts

- Most e-mail is insecure and it should be regarded as insecure and can be read by anyone unless it has been encrypted.
- E-mails are hard to destroy, they can be backed up and are recoverable.
- Most software used to operate networks, including web servers, mail servers and gateways, logs transactions and communications and may be stored on file servers
The Privacy Commissioners Position

- An organisation and its management has a responsibility for issuing instructions as to their proper use.

- The Federal Government has a light touch position on Privacy based on the National Privacy Principles for the Private Sector. Public sector must collect, store, process, disclose and dispose of personal information in accordance with the National Privacy Principles.

- Organisations are encouraged to foster an environment where staff are assured that the privacy of their communications will be respected as long as they abide by the organisation's stated policy. Policy or practice which leads staff to believe that their privacy in the workplace is not respected may have a negative impact on morale and productivity.
NSW Workplace Surveillance Act
Overview and Objectives
NSW Workplace Surveillance Act Overview

• Introduced in October 2005 and specifically relates to NSW Employers

• Specifies conditions how and in what circumstances NSW employers can conduct electronic surveillance of employees in the workplace.

• Relates to the surveillance of an employee by:
  – **Camera**: Monitoring or recording by camera visual images of activities on premises or in any other place
  – **Computer**: Monitoring or recording of computer information input, output or use by software or other equipment. (including, but not limited to, the sending and receipt of emails and the accessing of Internet websites)
  – **Tracking**: Monitoring or recording the geographical location or movement (such as a global Positioning System) by means of an electronic device

• Defines two types of surveillance Overt and Covert
Definitions

• **An Employee**
  A person employed in any industry, whether on a salaries or wages or piece-work rates. A person is not prevented from being an employee only because the person is working under a contract for labour only / substantially for labour only, the person works on a part time or casual basis, the person is the lessee of any tools or other implements of production, the person is an outworker or the person is paid wholly or partly by commission. An employee for the definition of inclusion in the act also includes volunteers.

• **At work** means where an employee is:
  At a workplace of the employer (or a related corporation of the employer) whether or not the employee is actually performing work at the time, or
  At any other place while performing work for the employer (or a related corporation of the employer).

• **Workplace** means premises, or any other place, where employees work, or any part of such premises or place.
Overt Surveillance Overview

- Must provide 14 days notifications
- Must explicitly define; how and when and where surveillance will be undertaken, the purpose of surveillance and the information collected
- Explicitly excludes restrooms, bathrooms, change rooms etc
- Must display warnings at every entry point at which surveillance is undertaken
- Data collected can only be used for the purpose that was notified
- Must not be used in a discriminate manner (age, sex, religion, ethnicity)
- Prohibits employees from stopping delivery of email unless it constitutes spam or is considered to be a harassment or a threat.
- Can not restrict union related email
Covert Surveillance Overview

• Can not undertake covert surveillance under any circumstance without the written authority of a covert surveillance authority (such as a magistrate).

• Data obtained through covert surveillance means can only be used for the purpose approved by the covert surveillance authority.

• A covert surveillance authority will only authorise covert surveillance if there is just cause to believe that there is a valid reason to believe that a wrong doing has occurred/ is occurring.

Incident Investigations – Undertaking investigations of serious incidents may be difficult to achieve in a timely manner through covert surveillance. It is better to proactively cover the potential for these types of surveillance through overt surveillance and notifications.
Monitoring Information Assets

Risks and Issues
Monitoring and Surveillance Issues

- **Unfair Dismissal Claims – Inadequate definition and communication of acceptable use** Increases the risk of unfair dismissal claims should an employee be dismissed for unacceptable use.

- **Uniform Understanding of and applicability** Acceptable Use - A light touch to defining acceptable use Such as a Broad Statement of “Email can be used for a reasonable amount of personal use” makes it difficult for employers to define, monitor and track acceptable use.

- **A heavy approach to monitoring can increase accountability risks.** For example, Installing an email monitoring system that filters objectionable material could leave the employer that much more responsible for any objectionable email that the system fails to prevent.
Finding the Balance

• What risks are we trying to prevent, detect or manage
• What policy is monitoring intended to enforce
• How can the policies be applied uniformly and consistently
• What data will be collected through monitoring activities
• For what purpose will the data be used
• How will the monitoring data be maintained, stored, classified and disposed.
IT, Privacy and Acceptable Usage

The NSW Workplace Surveillance Act formalises what any sensible employer should do to mitigate employee risks to information assets - establish a policy, educate employees about appropriate use and enforce the policy, with sanctions for breaches.

"The act simply says employers must tell staff that their use of employer provided equipment / facilities is being monitored. At the same time, staff must understand that if they use the web on their work computer and employer provided email to send private emails, there are systems in place to track and filter where they surf, and what they send."
Monitoring and Surveillance
Policy Requirements
Policy Requirements

• Enhance policies proactively. While it may not be law now it does mitigate immediate risks and puts the organisation in a better position for legislative changes.

• Ensure policies define clearly and completely; an employees requirements for the acceptable usage of Information Assets, and, the scope of monitoring, for what purpose the monitoring is undertaken and how the data obtained through monitoring activities will be used.

• Ensure policies are socialised in a way that it can be clearly demonstrated that a reasonable person would be aware of and understand them and Establish and maintain visual Signs of Surveillance Activities. (Login Screens, Posters, Entrances).
Policy Requirements

- Implement controls to enforce policies as consistently as practicable.
- Undertake surveillance and monitoring of employees and information assets in accordance with your policies.
- Maintain appropriate records of surveillance activities