# “Big brother”or vital risk management strategy?
## A practical guide to workplace surveillance

Michael Kay, Wallmans Lawyers
Scott Long, University of Adelaide

ACC Adelaide
1 March 2019

# In this session ….

Michael Kay will be summarising the law around surveillance and privacy in the workplace, how it works, and dispelling common myths

Scott Long will be providing practical examples around how surveillance is used at his workplace, and the day-to-day practical and legal considerations arising from its use

# #spoileralert

Surveillance *is* an essential risk management strategy for almost *all* employers

# What do we mean by “surveillance”?

- “listening” and “optical devices”: sound and video recording of still or moving images
- “data surveillance device”: monitoring internal and external e-mail, internet use, social media use, keystroke logging, keyword “flagging”
- “tracking device”: GPS in vehicle, mobile phone, RF technology on farms
- watch this space: bio surveillance - X-ray, thermal imaging, finger print?

# When should an employer undertake surveillance?

- Protection of assets
- Monitoring employee performance
- Monitoring employee behavior
- Work health and safety / duty of care
- Other legal compliance (security obligations ie Airport)
- More practical examples from Scott later……

# Key legal Considerations…

- Audio / video recording focused on prohibitions involving “private conversations” or “private activities”
- Express / implied consent (overt versus covert surveillance) is a paramount consideration underpinning the SD Act
- Two key exceptions in Act: lawful interest and public interest (but as Scott will elaborate on later, a complex and rarely tested exception, use with caution)

# Consent to be “surveilled” – what does this mean?

- Express or implied (express preferable, but may not be practicable)
- Employees: Express acknowledgement in contract of employment
- Employees: Addressed in a policy (ie NSW example)
- Large and visible warning signs, particularly where site visitors
- Pre-recorded advisory on telephone calls
- A “log-in” notice when employees log-in to their computer / device

# What about my “right to privacy”?

- Contrary to what is often alleged, there is *no* general right to privacy at law in or around the workplace
- Legislation (*Privacy Act, SD Act, criminal law)* offers protections only in particular circumstances (e.g employee record exclusion, illegal acts)
- Employer property (computers, vehicles, mobile phone), assuming compliance with SD Act, belongs to the employer.
- An employee has no right to insist on privacy or to limit access to information from those devices (despite objections otherwise)

# What does this mean for my workplace?

- This will depend on your workplace. Some examples……
- Eg: Employers who provide many with computer access should conduct comprehensive surveillance to minimise vicarious liability risk
- Eg: Employers who have frequent public access should consider CC TV to address safety and duty of care considerations
- Eg: Employers with a fleet on the road, should consider GPS to consider safety, but also assess efficiency and performance

# A practical case study

# The University of Adelaide

# Key University Surveillance tools

- Cameras
  - All 'public' spaces are captured
  - Capability to record audio, but *generally* not used
- IT Systems
  - Email tracking and active diversion
  - Usage logging: site access, web, messaging, SMS, business systems

# Why?

- What Michael said…

…but safety and wellbeing of all campus patrons is paramount

- Deter, detect and deal with inappropriate behaviour to foster campus as a safe community place.

- Make surveillance a positive message

# Welfare and Safety: Privacy is not always the trump card

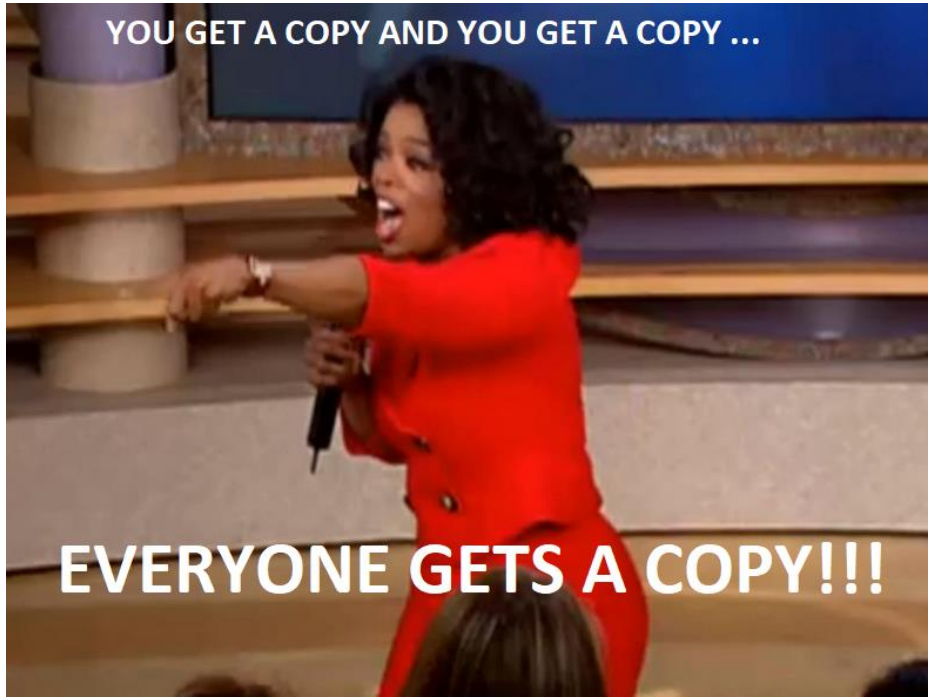
- Get familiar with the Privacy Act:
  - General Permitted Situations: *lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.*
  - APP 6 Disclosure Circumstances: *the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose*

- Legislative prohibition on visual recording is only for private activities - filming in a public place using a mobile telephone is ok… unless it's up someone's skirt.
- If someone is causing a nuisance, utilise your WHS obligations to move them on or call the police to do it for you!

# Welfare and Safety: Optical

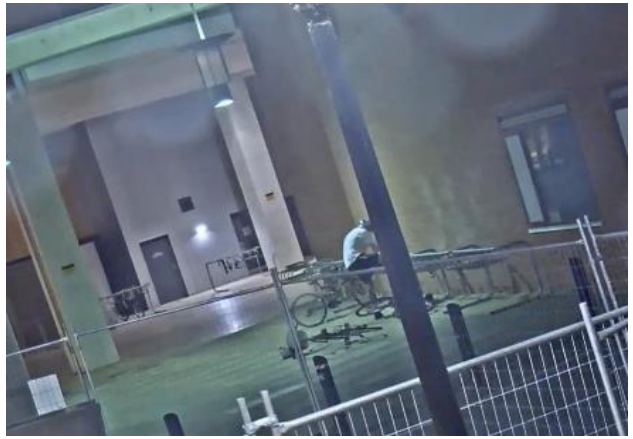
- *"The University collects Personal Information in a number of ways including… from CCTV cameras on University premises."* (Privacy Policy)

- Prohibition on visual recording is only for private activities – if they're in your space get them on film but…
  - ✓ Have clear signage
  - ✓ Be cautious about recording audio – consent issues
  - ✓ Understand who has access to camera systems
  - ✓ Control your security heroes!



# Optical Examples

- Contract dispute
- Building damage claim
- Underestimating intelligence



# Audio

- Generally, consent is required
- Recording without express consent is permitted if reasonably necessary for the protection of the lawful interest of that person
  - If someone is issuing threats, blackmail or trespass is reasonably suspected
  - Use with caution!  This is not a general permission to capture conversations
  - Document the process if a known surreptitious recording is going to take place
- For contentious situations (and difficult people) be clear and up front:
  - Suspected secret recordings: clearly advising all parties that you do not consent to being recorded – say it more than once!
  - Anticipatory incidents:  Clearly advising all parties that you intend to record and why.

# Email / IT

- "*Normal operation and maintenance of University IT includes logging of usage and activity on University IT. The University may monitor and analyse such logs… to meet the University's legal obligations.*" (IT Acceptable Use and Security Policy )
- What's yours is mine – emails sent to and from corporate systems are corporate property
- Your system as a weapon of war - email abuse is a threat to work health safety and welfare
  - *"You leave no alternative but for me to address matters directly, at a time of my choosing, to the staff in question. The effect this will have on them and their families will be largely due to your failure to take the matter seriously."*
  - 400+ emails sent over 20 days to the same recipients is not appropriate use
- Use your systems protect your organisation and your employees – e.g. email diversion
  - Note requirements of the *Telecommunications (Interception and Access) Act 1979* (Cth)
  - Have a process with a clear audit trail – identify the triggers, approvals, oversight processes

# Access by Third Parties

- Make sure who is asking is actually who they say they are!
  - Police – warrants of execution
  - Solicitors – formal letters / client consents / statutory declarations
  - *My father's life's work…* Court orders

- Establish a release protocol
  - Would the person reasonably expect the information to be released in the circumstances?
  - How contentious is the request / information?
  - Why does the requestor want it?

- Consider what role (if any) that your organisation wants to play in a dispute?
  - Crash and bash – scrutiny from insurers
  - Third party employment issues – scrutiny from unions
  - Unintended media / social media blowback
  - Burden of being a witness

- If all else fails - apply the Australian Privacy Principles

# CONTACTS / QUESTIONS

**Michael Kay**
Partner and Practice Leader, Workplace Relations, Employment and Safety
Wallmans Lawyers
Partner and Practice Leader
T: (08) 8235 3044
E: michael.kay@wallmans.com.au

**Scott Long**
Director, Legal Services
Legal and Risk, Division of University Operations
The University of Adelaide
T: +61 8 8313 8113 | F: +61 8 8313 4667
E: scott.long@adelaide.edu.au