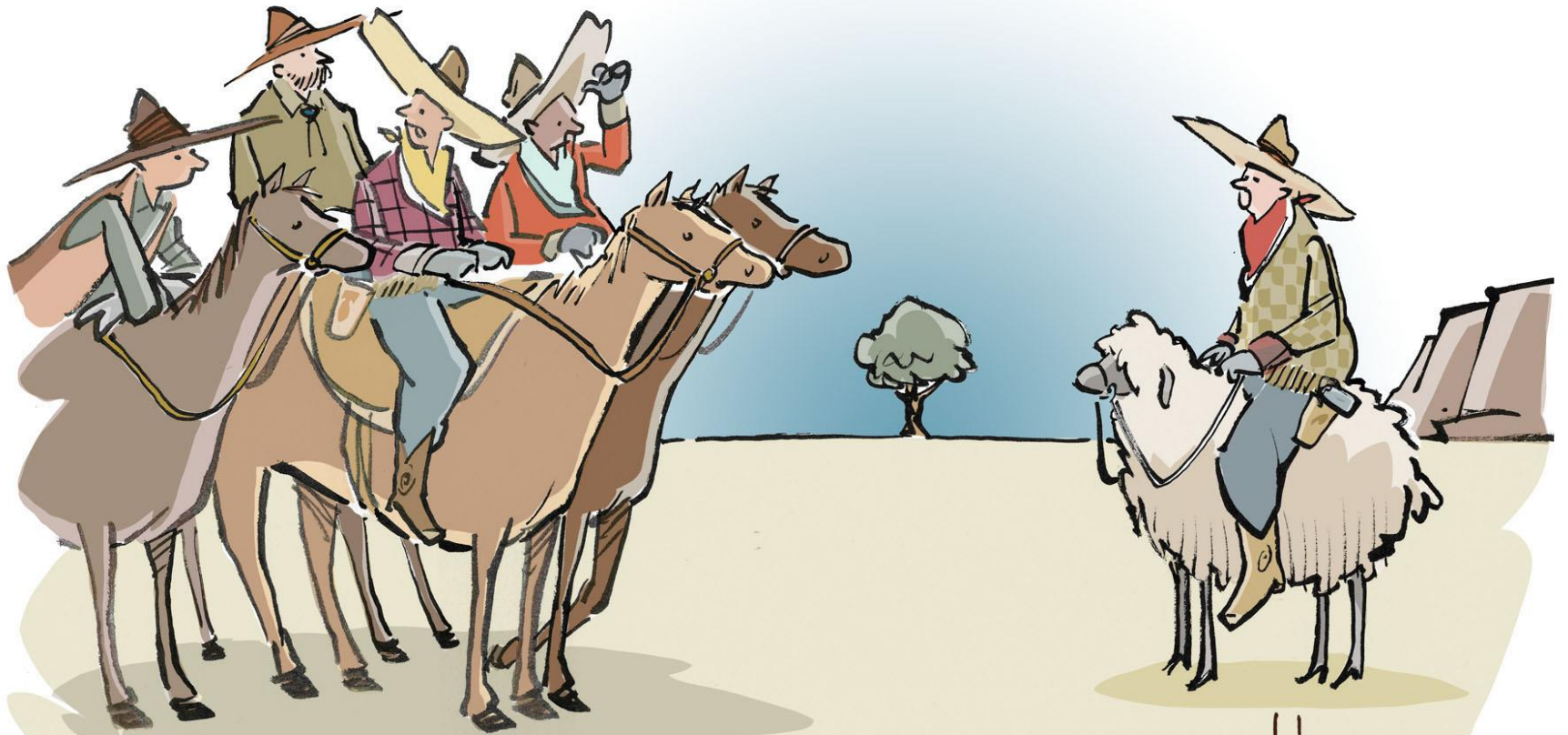


# Emerging trends in BYOD

**Arvind Dixit**  
**Senior Associate**  
Corrs Chambers Westgarth

[arvind.dixit@corrs.com.au](mailto:arvind.dixit@corrs.com.au)





"DO WE HAVE A BYOD POLICY?"

# Advantages / disadvantages

- Theoretical advantages of BYOD are:
  - Cost savings
  - Productivity
  - Employee satisfaction
- Major technical challenge is the fact that the perimeter of the organisation is blurred and more difficult to secure



# Data Security

## Confidential Information

- What confidential information do employees have access to?
- Possible breach of third party obligations
- Confidential Information is protected under common law if:
  - the information has the necessary quality of confidence about it; and
  - the circumstances in which the information was communicated or obtained gives rise to a relationship of confidence.
- The rise of “BYOC”

# Data Security

## Privacy

### APP 11.1

*If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:*

*(a) from misuse, interference and loss; and*

*(b) from unauthorised access, modification and disclosure.*

### APP 11.2

*If an APP entity...no longer needs the information...the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure the information is de-identified.*

# Liability issues

## Support and licensing

- Apportionment of liability between individual and the company
- Use of BYOD technologies could potentially breach licensing agreements company has with third parties
- Regulating use of apps/software on a personal device for work purposes where the company does not hold the licence rights

# Surveillance and interception

- NSW and the ACT have specific legislation governing **data surveillance by employers** (such as the monitoring of emails and use of devices)
- All Australian jurisdictions have Acts dealing with the **use of surveillance devices**
  - In some states (such as Vic and NSW) these acts make it unlawful for any person to install a tracking device to monitor the location of a person or an object (such as a BYO device) **without the express or implied consent** of that person or the person in lawful possession of the object
- It is an offence for an employer to **“intercept” any communication** (either voice, or text) that travels over a telecommunications system (including an internal telecommunications system)



# Governmental guidance

- Various Australian States, and governmental departments have issued “mobility” guidance
  - NSW government – Mobility Solutions Framework
  - SA government – Securing smart-phones and other portable storage devices
  - Qld government – Recordkeeping implications of mobile and smart devices
  - Dept of Defence – Risk Management of Enterprise Mobility Including BYOD
- Extent of overseas regulation and attitudes vary

# Shifting perceptions

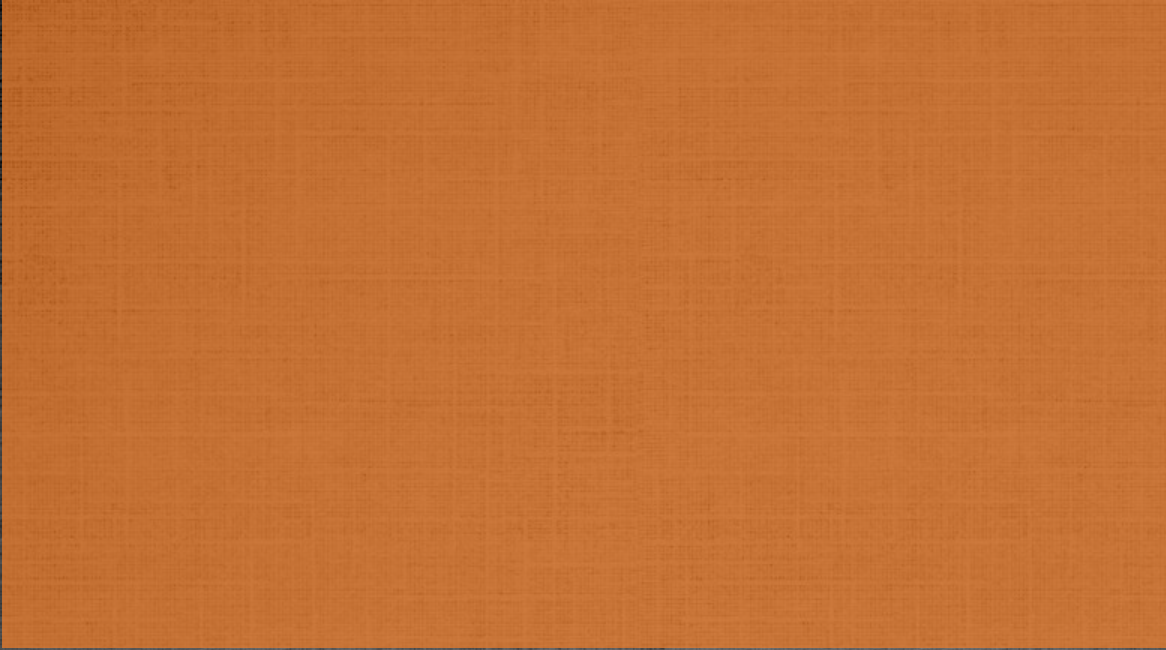
1. User error is the greatest risk factor

2. Security through technical innovation rather than regulation

# Shifting perceptions

3. Less is more in your BYOD policy

4. Remote wiping poses a large potential risk



**Arvind Dixit**  
**Senior Associate**  
Corrs Chambers Westgarth

[arvind.dixit@corrs.com.au](mailto:arvind.dixit@corrs.com.au)

**CORRS  
CHAMBERS  
WESTGARTH**

lawyers

ITechLaw Asia Pacific Conference - 27 February 2014

10451045/1