Cybersecurity and Personal Data – Can/Should We ‘Protect’ Our Privacy from the Next Breach?

Associate Professor Mark Burdon, QUT Law,

World Legal Summit, The University of Queensland,

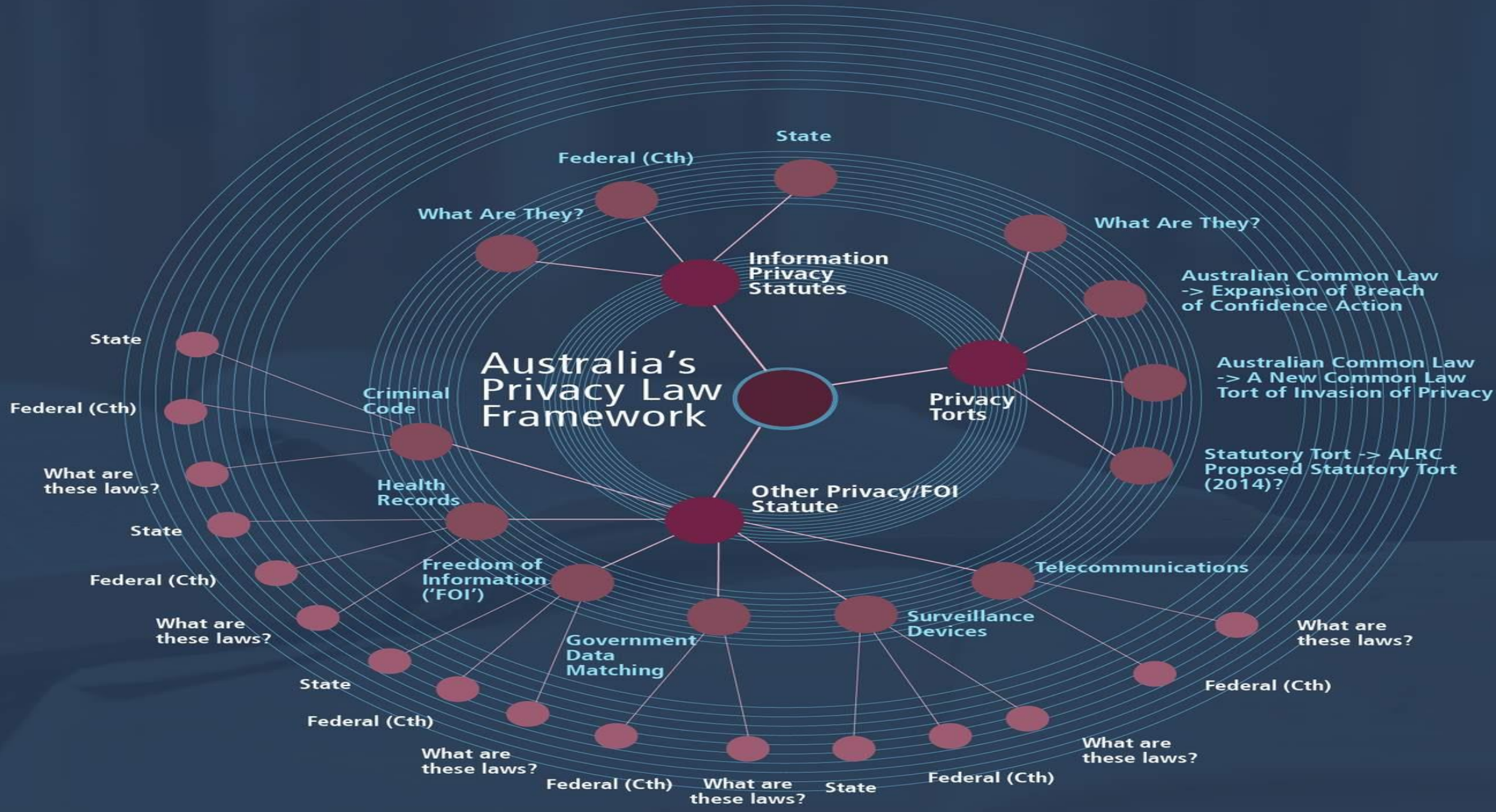
1 August 2019.

Introduction

- Does Australia have a cybersecurity law framework?
- How does the *Privacy Act* fit within that framework?
- What's reasonable security under Australian Privacy Principle 11?
- Do data breaches need to be notified under the *Privacy Act*?

Cybersecurity Framework

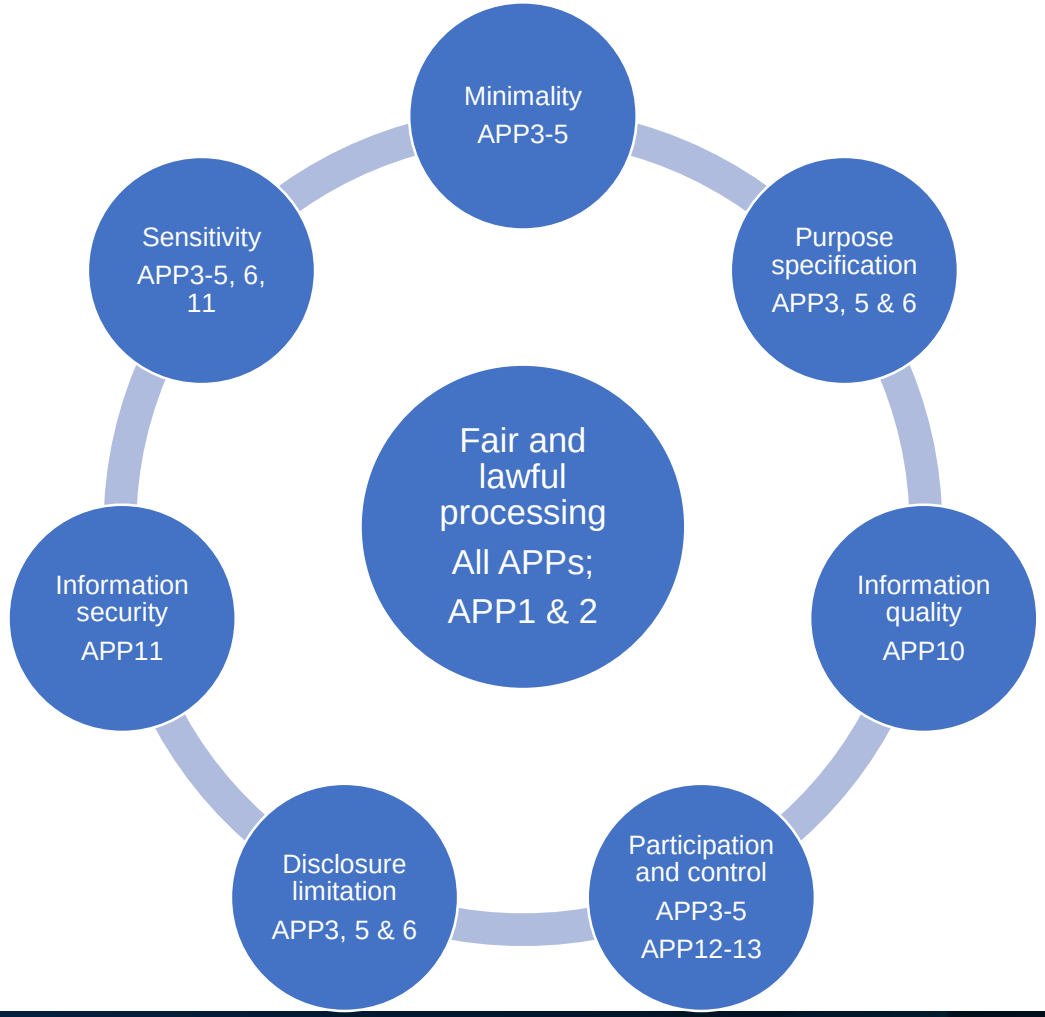
Cybercrime	• Cth Criminal Code – Hacking attacks; denial of service attacks; malware attacks; possession of hacking tools; identify theft/fraud; electronic theft
Protection of critical infrastructure	• *Security of Critical Infrastructure Act 2018* (Cth); *Telecommunications and Other Legislation Amendment Act 2017 (*Cth)
Telecommunications operation	• *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth)
Cybersafety	• Cyberbullying, non-consensual sharing of intimate images
Sector specific guidelines	• APRA Prudential Standard CPS234; Protective Security Policy Framework; Information Security Manual
Information privacy law	• Federal/state-based laws; data breach notification; some sector specific requirements


Australia's Privacy Law Framework
Information Privacy Statutes
State
Federal (Cth)
What Are They?
Privacy Torts
What Are They?
Australian Common Law -> Expansion of Breach of Confidence Action
Australian Common Law -> A New Common Law Tort of Invasion of Privacy
Statutory Tort -> ALRC Proposed Statutory Tort (2014)?
Other Privacy/FOI Statute
Criminal Code
State
Federal (Cth)
What are these laws?
Health Records
State
Federal (Cth)
What are these laws?
Freedom of Information ('FOI')
State
Federal (Cth)
What are these laws?
Government Data Matching
Federal (Cth)
What are these laws?
Surveillance Devices
State
Federal (Cth)
What are these laws?
Telecommunications
What are these laws?
Federal (Cth)

Privacy Act 1988 (Cth) - Overview

- Embodies a ‘principled approach’
  - Sets broad principles to be applied
  - Gives fair degree of discretion to implementing bodies
  - Technology neutral
- Does not accord privacy rights to individuals
  - Provides rights of limited involvement in process of personal information exchange
  - Sets minimum obligations for entities
- Focus….
  - Imbuing a sense of lawfulness and fairness in personal information exchange processes

The Australian Privacy Principles (APPs)



APP 11

- 11.1 entity holds personal information, the entity must take ***such steps as are reasonable in the circumstances*** to protect the information from:
  - Misuse, interference and loss; and
  - Unauthorised access, modification and disclosure

- 11.2 regards the destruction or de-identification of personal information that is held, but no longer needed for use or disclosure purposes
  - Unless
    - Personal information is not a Commonwealth record
    - Not required to retain under an Australian law

APP 11 – Core components

Six key security considerations

- *Misuse* – used for a purpose not permitted by the Privacy Act
- *Interference* – hacking attack that leads to exposure
- *Loss* – physical or virtual
- *Unauthorised Access* – accessed by an individual without permission
- *Unauthorised Modification* – altered without permission
- *Unauthorised Disclosure* – accessible or visible to others or releases from control

What are Reasonable Steps?

- APP 11 is representative of PBR
  - Set broad principles; up to organisations to interpret
    - Flexibility on implementation
    - Reasonable requirement is contextual
    - Light touch approach

- APP Guidelines
  - Shape understanding of implementation boundaries
  - Highlights what is reasonable in terms of security related activities
  - Broad parameters of what constitutes reasonable security

What are Reasonable Steps?

- Nature of the entity holding the personal information
- Nature and quantity of personal information held
- Adverse consequences
- Practicality of implementing information security
- Privacy invasiveness of the measure

Regulatory Parameters

- OAIC decisions re information security:
  - Nature of the entity
    - *Vodafone OMI*
  - Quantity and sensitivity of held data
    - *Department of Immigration and Border Protection: OMI [2014]; Telstra Corporation Limited: OMI [2014]; 'BO' and AeroCare Pty Ltd* [2014]
  - Practicality of implementation
    - Dell/Epsilon OMI; *AAPT and Melbourne IT OMI*

Damages

- Damages are available under the Act
  - s 52(1A)
    - The complainant is entitled to a specified amount by way of compensation for any loss or damage suffered
  - s 52(1)(b)(iii)
    - Damages are not limited to economic loss
    - Non-economic loss; aggravated
    - “includes injury to the complainant's feelings or humiliation suffered by the complainant”

- 2014 Reforms - enhanced powers
  - ss13G, 80U and 80W - Civil penalties for serious or repeated infringements
  - s33E - Enforceable written undertakings
    - Take specific action;
    - Refrain from action or won’t act in interference of privacy
  - Compliance audits – private sector organisations
  - Make determinations following CIIs

Award of Damages

- 2010/2011 – 243 complaints that led to remedies
  - 19 – payments under $1,000
  - 14 - payments from $1,000 - $5,000
  - 1 – payment from $5,000 - $10,000
  - 1 - payment over $10,000

- Post 2011 and 2014
  - *QF and Spotless* [2019] - $60,000/$6,000
  - *LB and Comcare* [2017] - $23,000
  - *LU and Dept. of Defence* [2017] - $23,000
  - *'DK' and Telstra Corporation Limited* [2014] - $18,000
  - *'CM' and Corporation of the Synod of the Diocese of Brisbane* [2014] - $7,500
  - *'BO' and AeroCare Pty Ltd* [2014] - $8,500
  - *'CP' and Department of Defence* [2014] - $5,000

Notification Data Breach Scheme

Notification Triggers

- **Acquisition**
  - Low ‘triggering threshold’
    - Notify on breach or belief of breach
    - Notify even if no evidence of personal information acquired
  - *Ex ante* focus
    - Threat to improve security measures
    - Reputational sanction
  - Consumer oriented
    - Individuals are made aware of potential data breaches
    - Take action to mitigate potential harms

- **Risk-based**
  - Higher ‘triggering threshold’
    - Notify where a risk assessment identifies a risk of harm
    - Different standards in operation
  - Ex post focus
    - Target problem; minimise notification
    - Notification fatigue
  - Business oriented
    - Breached organisation determines whether harm arises

s26WA *Privacy Act*

- Three key components

  1. An unauthorised access or disclosure, or a loss, of personal information
  2. Likelihood of resulting in serious harm to one or more individuals
  3. Remedial action prevents the risk

- What is a serious harm?
  - Serious harm is not defined - factors
    - The type and sensitivity of information
    - The nature of the potential harm
    - Who gained access to the breached information.
  - Harm is construed broadly
    - Financial, physical, emotional and reputational harms

Report at a glance

Entities regulated by the Privacy Act should review this report and use the learnings to enhance their prevention and response strategies for the benefit of all Australians. One of the key messages that we take from this inaugural review of the NDB scheme is that entities must put individuals first.

Number of eligible data breaches

Total data breach notifications under the NDB scheme from 1 April 2018 to 31 March 2019

964

712%

Increase in notifications since the introduction of the NDB scheme

Total data breach notifications compared with the previous 12 months under the voluntary scheme

Data breaches that were malicious or criminal attacks

Malicious or criminal attacks were the main sources of data breaches in the NDB scheme's first year

60%

153

Number of breaches attributed to phishing

Phishing and spear phishing continue to be the most common and highly effective methods by which entities are being compromised

Cyber incidents where credentials were obtained by unknown means

The notifying entity wasn't aware of how the credentials were obtained, because they had not detected any phishing-based compromise

28%

83%

Data breaches that affected fewer than 1,000 people

The vast majority of data breaches reported in the first year of the NDB scheme each affected fewer than 1,000 people

Data breach notifications attributed to human error

Many data breaches involved human error, such as through unintended disclosure of personal information or the loss of a data storage device

35%

55%

Health sector data breaches due to human error

Human error was the leading cause of data breaches in the health sector, compared with an average of 35% for all sectors

Finance sector data breaches due to human error

In the finance sector, human error accounted for 41% of data breaches, compared with an average of 35% for all sectors

41%

86%

Notifications that involved contact information disclosure

Contact information was the most common form of personal information disclosed through data breaches during the period

Summary

- Largely fragmented legal structures
  - Cybersecurity and privacy
- *The Privacy Act's* principles-based framework
  - Delegates significant responsibility to regulated entities
  - APP 11 – reasonable security
- Primary policy vector (?)
  - Enhance organisational security of personal information through NDB scheme; rather than complaint mechanisms or civil penalties
- Which begs the question….

Can/Should We ‘Protect’ Our Privacy from the Next Breach?

- **Discussion Panel**

  - Nicole Murdoch
    - Principal, EAGLEGATE Lawyers; Director, Australian information Security Association; Member, QLS Cybersecurity Working Group
  - Daniel Pearson
    - Adviser - General Insurance, Findex Insurance Brokers Pty Ltd
  - Kim Trajer
    - Chief Operating Officer, McCullough Robertson Lawyers and Member, Queensland Law Society Innovation Committee
  - David Williams
    - Managing Director, FinTechnology