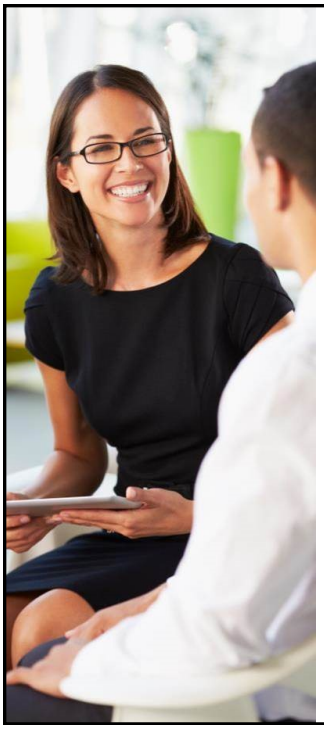
Baker McKenzie.

Privacy Law Update

Briefing for Eastern Suburbs Law Society

25 August 2018

Patrick Fair
Baker McKenzie



Outline of presentation

1 Privacy Fundamentals

What is privacy law?

- A legal framework that regulates the collection, disclosure use and management of information and opinions about people (**personal information**).
- To be regulated the information or opinion must be about a natural person a person that is identified or identifiable.
- Information is regulated whether it is true or not, no matter how it is stored and whether or not it is in the public domain.
- Federal and state legislation.
- Federal law covers express subject matter inclusions: tax file numbers, credit reference information, metadata held by Telcos.
- Federal law has conditional exclusions for small business, political parties, employees, the media, emergencies, law enforcement.
- Also extensions to include those trading in personal information, health service providers and parties contracting with the Commonwealth.

Sensitive Information

- Need consent to collect sensitive information
- Restrictions on : any secondary purpose must be directly related to the purpose of collection
- Cannot be used for direct marketing without consent

Categories of sensitive information		
racial or ethnic origin	political opinion	political membership
religious belief	religious affiliation	philosophical belief
membership of a professional or trade association	sexual orientation	criminal record
health information	genetic information	biometric information for identification

Australian privacy principles (APPs)

Category	Key obligations	APP
Privacy compliance and transparency	Maintain systems and procedures to ensure compliance and publish a privacy policy which reflects privacy practices	APP 1
Collection	Collect PI only as reasonably necessary for activities and only from the individual unless impracticable	APP 3
Collection notice	Compliant collection notice at or before the time of collection (or as soon as possible after, if that is not reasonably practicable)	APP 5
Use and disclosure	Use/disclose PI only for the primary purpose for which it was collected, or for a related purpose that individual would reasonably expect, or with the individual's consent; special requirements for direct marketing outside Spam and telemarketing context	APP 6, 7
Offshore disclosure	Take reasonable steps to ensure recipient does not breach APPs or other options. Deemed liability for any breach by recipient	APP 8
Quality + security	Keep PI accurate, complete and up-to-date; take reasonable steps to secure and protect PI; destroy or de-identify PI once no longer needed	APP 11
Access and correction	Give access and make correction within reasonable period (30 days) of request, except in certain circumstances	APP 12, 13

Australian Privacy Principle 11.1

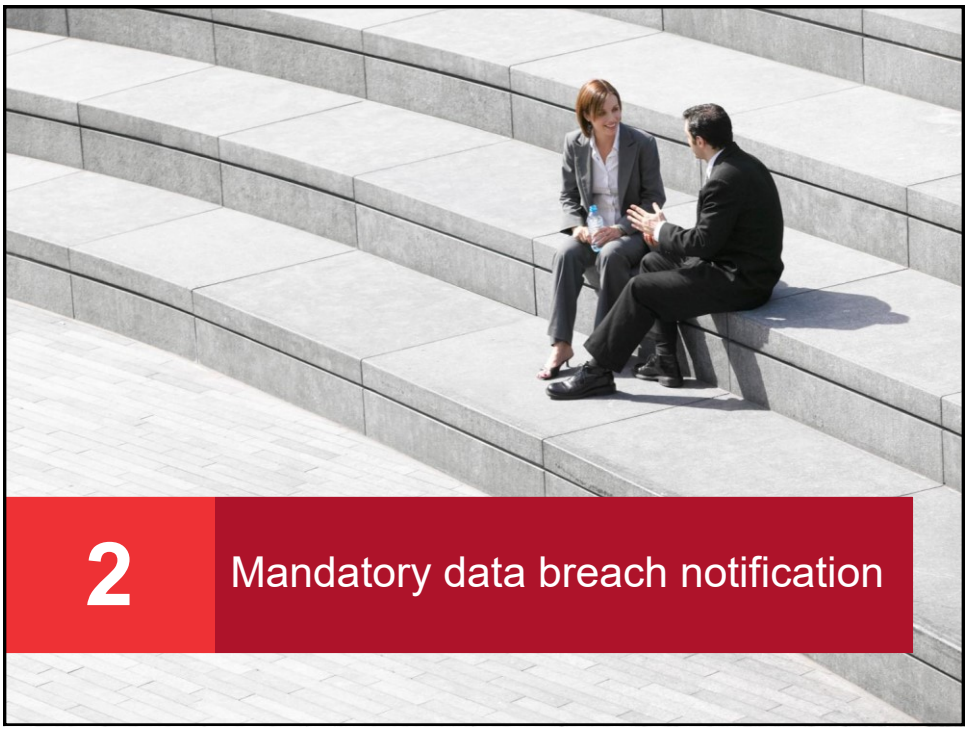
If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

Enforcement and penalties

- Failure to comply is unlawful interference with the privacy of an individual
- Investigations and publication of results, binding determinations (including compensation) and enforceable undertakings
- A contravention of these provisions is deemed an "interference with the privacy of an individual" (new 13(4)(A) making a failure to comply subject to a civil penalty under 13G: maximum 2000 penalty units ($420k))
- Maximum is 5 x for body corporate ($2.1m)
- There is a right of appeal to the Administrative Appeals Tribunal in relation to the Privacy Commissioner's decision to:
  - refuse an application for exception; or
  - to issue a direction
- Potential for a representative complaint under section 38 of the Privacy Act.



2 Mandatory data breach notification

Key elements of the MDBN law

- Applies to "Personal Information" under the Privacy Act
- Does not amend the security obligation in APP 11.
- Covers:
  - suspected breaches: an obligation to investigate; and
  - unauthorised access, disclosure or loss.
- Notification duty arises if a reasonable person would consider that "serious harm" is likely.
- You may take action to remediate a breach.
- Notice to the Commissioner must be "as soon as practicable"
- Failure to comply is an unlawful interference with the privacy of an individual.
- Commenced 22 February 2018

MDBN Regime

What is "serious harm"?

- "serious harm" is not defined in the Act
- The EM says this at paragraph 41:
  - "Potential harms, depending on the circumstances, could include physical, psychological, emotional, economic and financial harm, as well as harm to reputation. …"
- The EM says at paragraph 42:
  - "Part IIIC is expected to predominantly require notification of eligible data breaches where a reasonable person would conclude that there is a likely risk of serious financial, economic or physical harm to individuals. However, the likelihood of other kinds of serious harm… cannot be ruled out, especially for eligible data breaches involving health information, other forms of 'sensitive information'…"

MDBN Regime

Matters relevant to whether serious harm is likely

- Further, section 26WG requires a consideration of the kind or kinds of information in determining whether a disclosure is likely to result in serious harm:
  - the sensitivity of the information
  - whether the information is protected by security
  - whether security measures might be overcome
  - whether a security technology or methodology was used and the likelihood it might be circumvented
  - the persons or kinds of person who have obtained the information
  - the nature of the harm

3 Developments of interest

Developments

Developments of interest

- General Data Protection Regulation (**GDPR**) became law in the EU on 25 May 2018:
  - expands and extends privacy regulation
  - can apply to Australians and Australian businesses
- Consumer Data Right is under consultation:
  - Initially for the banking industry
  - Treasury Laws Amendment (Consumer Data Right) Bill 2018
  - Consultation closes 7 September 2018
  - https://treasury.gov.au/consultation/c2018-t316972/


Questions and discussion?