Are you prepared for the new privacy law?

Industry briefing 11 December 2013

Presenter: Patrick Fair

Partner

Overview

Overview

- Background to the amendments
- Privacy fundamentals
- The current law
- The law from 12 March 2014
- Significance of the changes

Background

Thailand: Draft law sent to Parliament in 2012

India: The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

Taiwan: PDPA 2010 in effect from 1 October 2012

Malaysia: PDPA 2010 (date for coming into force yet to be set)

Singapore: PDPA passed 15 October 2012; sunrise period until 2/1/14 and 2/7/14

Vietnam: Provisions spread across the Civil Code, the IT Law, the Penal Code and the Telecommunications Law.

South Korea: Personal Information Protection Act 2011

China: Provisions regulating Internet Information Services/

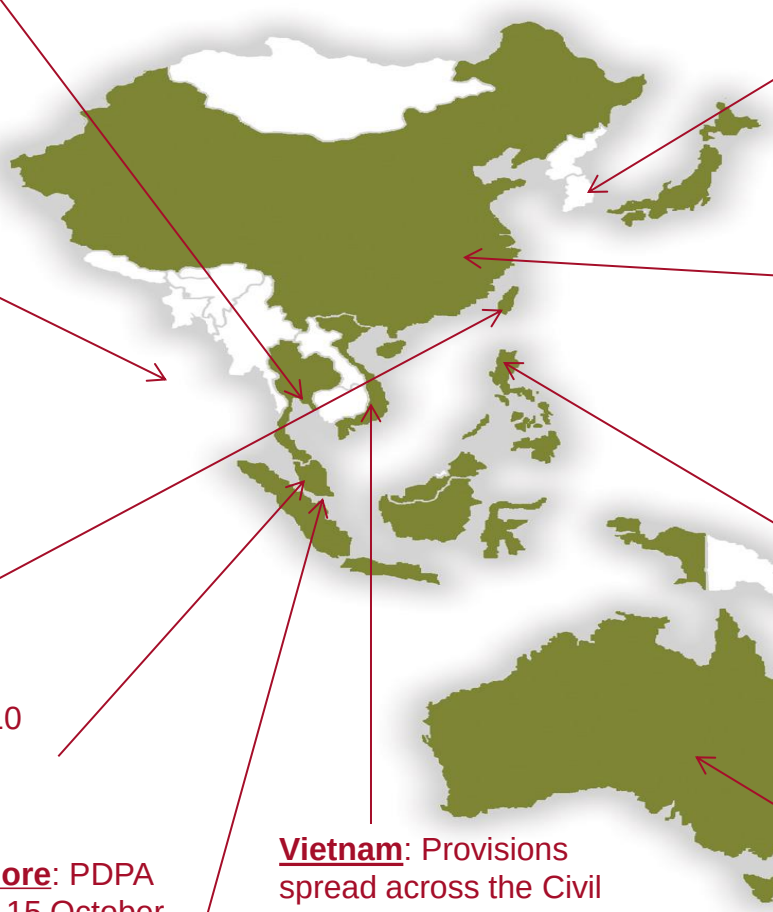
NPC Decision on strengthening the protection of internet information

Hong Kong: Personal Data (Privacy) Amendment Ord (amendments in full effect on 1/4/2013)

Philippines: Data Privacy Act (August 2012)

Cybercrime Prevention Act (September 2012)

Australia: Amendments come into effect in March 2014



Australian law reform

- OPC review 2005
- ALRC consultation and report 2006 – 2008
- Australian Government Response 2009
- Draft revised privacy legislation 2010-2011
- Bill introduced 2012
- Bill passed **29 November 2012**
- 2012 Act

Privacy fundamentals

Privacy Law Framework

- Regulates the handling of “Personal Information” by an “organization”
- Does not apply to organizations with gross turnover <$3m unless:
  - Contracting with the commonwealth
  - Dealing in personal information
  - Dealing with health information
  - A media origination that subscribes to a code of practice
  - A political party
- Employee records are exempt.
- A higher standard applies to “sensitive information”.
- Special rules apply to credit reference information and tax file numbers

What is “Personal Information” now?

- Defined as:

  "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion".

- No requirement that is information be “private”
- Personal information can be information freely available in the public domain

What is “Sensitive Information”

(a) information or an opinion about an individual's:

(i) racial or ethnic origin;

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual preferences or practices; or

(ix) criminal record;

that is also personal information; or

(b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.

Current law

Existing regime

- 2 set of principles: NPPs (private sector) and IPPs (public sector)
- 10 NPPs apply to business
- loosely expressed: not prescriptive
- limited enforcement powers

Law from 12 March 2014

Key changes

- consolidated Australian Privacy Principles (APPs) (Schedule 1) replace NPPs and IPPs
- APPs have prescriptive elements
- new provisions on credit reporting (Schedule 2) and privacy codes (Schedule 3)
- new enforcement powers (Schedule 4)

New definitions

- "APP Entities"= organisations and agencies
- "Personal information": information or an opinion about an identified individual, or an individual who is reasonably identifiable:
  - whether the information or opinion is:
    - true or not; and
    - whether the information or opinion is recorded in a material form or not.
- "Sensitive information" now includes biometric information

Australian Privacy Principles

- Divided into 5 Parts based on information life cycle: openness and transparency → collection→ handling→ integrity , access and correction.
- Key new requirements:
  - privacy policies / collection statements
  - compliance with you policy
  - unsolicited personal information
  - direct marketing
  - overseas disclosures

APP1: open & transparent management of PI

- Clearly expressed & up to date privacy policy:
  - **what** is collected
  - **how** it is collected and held
  - for what **purpose(s)**
  - **access** and **correction***
  - **complaints** procedure*
  - likelihood of **overseas disclosures**
    - must give details of countries if practicable*
- Implement systems / practices / procedures to ensure compliance*

* = new requirement

APP 3: Collection of Personal Information

- Distinction: non-sensitive v sensitive
- Non-sensitive:
  - must be reasonably necessary for one or more of the APP entity's functions or activities
  - for agencies, can also be directly related to one or more of the agency's functions or activities
- Sensitive:
  - Additional requirement for consent OR
  - One of the exceptions applies...

AAP 3: the exceptions use a defined term...

- "permitted general situation"
  - lessen or prevent serious threat to health
  - appropriate action in relation to unlawful activity etc
  - locate a missing person…
  - others
- "permitted health situation"
  - necessary for health services
  - necessary for administration or research
  - others
- non-profit organisation:
  - relates to activities of the organisation
  - relates to members or persons with regular contact

APP 6: Use or disclosure

- APP 6.1: PI held for primary purpose cannot be used / disclosed for secondary purpose unless:
  - individual consents or
  - specific exceptions apply
- APP 6.2: exceptions
  - reasonably expected = related or directly related
  - permitted general situation
  - permitted health situation
  - others
- APP 6.3: exception for biometric information / templates sent to enforcement bodies

APP 7: Direct Marketing

- **Not applicable** if Spam Act / Do Not Call Register Act applies
- APP 7.2: PI collected from the individual **and** reasonable expectation that PI will be used for DMs:
  - must provide simple means of opt out, and
  - individual must not have opted out
- APP 7.3: PI not collected from individual **or** no reasonable expectation that PI will be used for DMs:
  - must obtain individual's consent (unless impracticable),
  - provide a prominent opt out in each DM, and
  - individual must not have opted out
- Sensitive PI: consent is *always* required

APP 8: Cross-border disclosure

- APP8.1: Before disclosure, must take reasonable steps to ensure overseas recipient does not breach APPs (e.g. appropriate contract clauses, due diligence)
- s.16C: APP entity liable for acts of overseas recipients!
- Exceptions:
  - at least substantially similar protection overseas
  - warning and consent
  - other exceptions (similar to APP3 / 6.2)

Key issue: “disclosure” vs. “use”

- The OAIC defines “disclosure” taking place when an APP entity releases personal information from its “effective control”.
- Draft guideline says in “limited circumstances” providing personal information to an overseas contractor to perform services may be a use not a disclosure.
- Factors:
  - APP Entity maintains control over data
  - Data is secured from third party access
  - contractor has no independent right of use
  - Contractor must impose same obligation its contractors
- Routing data through foreign servers may be an example of “use’.

APPs 9 -13

- APP 9: restrictions on using government related identifiers
- APP 10: quality of information (ensure information collected, used or disclosed is accurate, up-to-date, complete and relevant)* more extensive
- APP 11: security of information (protection from misuse, interference, loss & unauthorised access etc.) & destruction / de-identification of PI if no longer needed* more extensive
- APP 12: giving individuals access to PI
- APP 13: correction of PI (30 day turnaround for agencies)

APP Codes

- Similar process for development of APP code to process for CR code
- Once registered, an APP code is enforceable and takes the place of the APPs
- APP codes may increase the compliance burden:
  - can go beyond APPs
  - exempt acts can be rendered subject to the Privacy Act

Enforcement

- Commissioner's powers:
  - Guidelines
  - Vary registered APP Codes
  - Investigations following complaints or on own initiative
  - Prosecution in Federal Court / Fed. Magistrates Court
  - Monetary penalties of up to:
    - $340,000 (non-corporate entities / individuals)
    - **$1.7million** (corporations)

Significance of the changes

Significance of the Reforms

At least the following steps are required:

- update privacy policies, notices and websites
- review / audit current practices
- implement improved procedures and systems for compliance
- training regarding the updated framework
- reflect changes in new contracts / amendments with data processors (on- and off-shore)

Questions and discussion

Contact: Patrick Fair

patrick.fair@bakermckenzie.com

(02) 89225534