# Privacy Reform

Trenton Schreurs, McInnes Wilson Lawyers
Bronwyn Furse, Thomsons Lawyers
Chair: Veronica Jumeaux, HWL Ebsworth Lawyers

# Format

- What is the current privacy landscape in Australia?
- An outline of the reform to the *Privacy Act*;
- Penalties for privacy infringement;
- Key changes following reform of the *Privacy Act* and tips and traps for the franchising industry;
- Recommended action for privacy compliance and compliance tips.

# Privacy Protection

- Currently regulated in a fragmented sphere;
- Dominant legislation is the *Privacy Act 1988* (Cth);
- The *Privacy Act* regulates and provides for what 'agencies' and 'organisations' can and cannot do with respect to the personal information of an individual;
- What then is personal information?

# Privacy Protection

- Personal information is broadly defined under the *Privacy Act* –necessarily broad;
- The *Privacy Act* is not the only legislation in Australia that discusses regulation of personal information – there is a federal piecemeal regime;
- Primarily the *Privacy Act* regulates 'organisations' through the application of the National Privacy Principles ('NPP's).

# Application of the Privacy Act

- Organisations vs. small business operators;
- Annual turover of < $3 million that does not:
  - Provides a health service;
  - Discloses personal information for a benefit, service or advantage;
  - Is not a contracted service provider to the Commonwealth.

# Privacy Protection – NPP's

- NPP1. Collection
- NPP2. Use and Disclosure
- NPP3. Data Quality
- NPP4. Data Security
- NPP5. Openness

# Privacy Protection – NPP's

- NPP6. Access and Correction
- NPP7. Identifiers
- NPP8. Anonymity
- NPP9. Transborder Data Flows
- NPP10. Sensitive Information

# Reform of Privacy Protection

- Attitudes about privacy protection have waxed and waned;
- In 2006, an inquiry was launched by the Australian Law Reform Commission (ALRC) into the potential and recommendations for reforming the *Privacy Act*;
- Following extensive consultation, the ALRC published their recommendations, some of which have been and will be implemented by March 2014.

# Reform of Privacy Protection

- Unification of the privacy principles;
- Recommended removal of the small business exemption;
- Recommended removal of the employee records exemption;
- Streamlining investigation and prosecution by the OAIC;

# Reform of Privacy Protection

- Compulsory data breach notification;
- More stringent credit reporting provisions;
- Requiring overseas levels of protection to the level of Australian protection when transferring personal information overseas;
- Consideration of a statutory cause of action for serious invasions of privacy.

# Reform of Privacy Protection

- Presently some reform recommended by the ALRC has been enacted;
  - Enhanced powers of the OAIC;
  - Changes to credit reporting laws;
  - The Australian Privacy Principles.

# Reform of Privacy Protection

- Organisations may still need to comply with data breach notification laws come March 2014;
- Other reform recommendations have yet to be considered.

# Penalties for Infringement

- Presently, limited by the *Privacy Act* and the powers of the OAIC;
- In March 2014, will become more substantial:
  - Monetary penalties from $340,000 to $1.7 million;
  - Enforcement of civil undertakings;
  - Civil penalty from FC or FMC;
- Ongoing potential for statutory cause of action or common law cause of action dependent on jurisdiction.

# Australian Privacy Principles

- **APP 1** – open/transparent information management (NPP 5)
- APP 2 – anonymity/pseudonymity (NPP 8)
- APP 3 – collection of personal information (solicited) (NPP 1)
- **APP 4** – receiving personal information (unsolicited) (NPP 1,2,4)
- APP 5 – notification of collection (NPP 1)
- APP 6 – use/disclosure (NPP 2)
- **APP 7** – direct marketing (NPP 2)

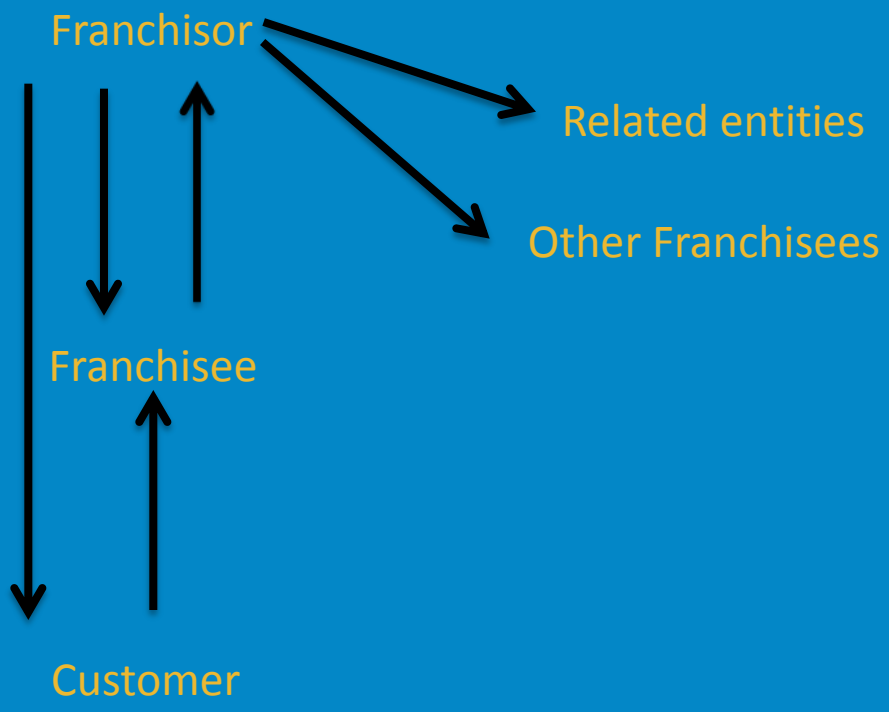
# Australian Privacy Principles

- **APP 8** – cross border disclosures (NPP 9)
- APP 9 – Government identifiers (NPP 7)
- APP 10 – quality of personal information (NPP 3)
- APP 11 – security of personal information (NPP 4)
- APP 12 – access to personal information (NPP 6)
- APP 13 – correction of personal information (NPP 6)

# Key exemptions

- Exempt particular acts and practices from compliance with the APPs
- Key exemptions
  - small business exemption
  - related bodies corporate exemption
  - employee records exemption

# Flow of personal information



# Key changes

- APP 1: Proactive privacy compliance programs
- APP 1: Privacy policy content
- APP 4: Unsolicited information
- APP 7: Direct marketing
- APP 8: Liability for offshore disclosures
- APP 13: Correction of personal information

# APP 1: Internal Privacy Compliance Program

- An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions and activities that will:
  - ensure the entity's compliance with the APPs
  - enable entity to deal with complaints and queries from individuals about the entity's compliance with the APPs

# Practical Steps

- Review information life cycle throughout the network
- Undertake a risk assessment to identify risks and compliance issues
- Review and update practices and procedures
- Update Privacy Compliance Manual
- Undertake compliance training

# APP 1: Privacy Policies

- Must be up-to-date and available free of charge
- New prescribed content for privacy policy
  - The kinds of PI that is collected and held
  - Purposes for which PI is collected, held, used and disclosed
  - How the PI is collected and held
  - How to seek access or correction
  - How to complain about a breach of APPs
  - How complaints will be handled
  - Likely offshore disclosures (where practicable, list countries)

# APP 5: Privacy Collection Statements

- Additional content for privacy collection statements:
  - Additional information where collection from a third party collection/where individual is otherwise unaware
  - Details of any law or court/tribunal order that requires or authorises the collection of personal information
  - Privacy policy sets out how to:
    - seek access or correction
    - complain about a breach of APPs and how such complaints will be handled
  - Likely offshore disclosures (where practicable, list countries)

# Practical steps

- Review information life cycle throughout the network
- Update the Privacy Policy
- Update all Privacy Collection Statements
  - Franchise Application Form
  - Prospective employees
  - Customers
  - etc

# APP 4: Unsolicited Information

- New assessment requirements for unsolicited information
- Requirement linked to collection
- Within a reasonable period of collection, must assess whether collection is permissible under APP 3 and then either:
  - destroy or de-identify; or
  - retain and handle in accordance with the APPs.

# Practical steps

- Identify sources for “unsolicited” personal information
- Develop policies and procedures for prompt review of “unsolicited” personal information

# Direct Marketing

- APP 7: Use and disclosure for direct marketing is not permitted unless an APP 7 exception applies
- No overlap with *Spam Act & Do Not Call Register Act*
- Various APP 7 exceptions
  - Sensitive information
  - Other types of personal information

# Direct Marketing

- Personal information (other than sensitive information) can only be used for direct marketing:
  - with consent
  - if collected from the individual, if direct marketing is:
    - within their reasonable expectations + opt out mechanism
    - not within reasonable expectations but impracticable to obtain consent + opt out mechanism + statement
  - if collected from a third party
    - impracticable to obtain consent + opt out mechanism + statement

# Practical steps

- Develop procedure for actioning:
  - Opt outs for direct marketing
  - Opt out of third party disclosure
  - Source requests
- Review and update direct marketing practices, policies and procedures

# APP 8: Offshore Disclosures

- Regulates offshore 'disclosures' rather than 'transfers'
- Under APP 8.1 prior to an offshore disclosure:
  - *take reasonable steps in the circumstances to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information*
- New liability for acts of overseas recipient
- Various exceptions to liability

# Practical steps

- Prior to transferring information offshore:
  - include suitable contractual obligations
  - consider any applicable liability exceptions
- Review and update existing arrangements

# Overview of practical tips

- Review and amend:
  - Review information life cycle throughout the network
  - Internal privacy practices
  - Marketing practices
  - Privacy policy, privacy collection statements
  - Privacy clauses
  - Contractor/franchisee privacy practices
  - Off-shore arrangements
- Update Privacy Compliance Program and Manual
- Undertake compliance training