Bartier Perry

30 August 2013

Norman Donato – Executive Lawyer

Navigating the Changing Privacy Landscape

A presentation for The Commercial Law Association Limited

Outline

- Snapshot of relevant legislation
- Why the changes?
- The APPs
- Some of the requirements
- Identity v Identification
- PI Tests
- IT today – Big data
- More Tests
- How do you avoid collecting PI today?
- Challenges before March 2014

Snapshot of relevant legislation?

- **Commonwealth Legislation**

  (Handling of PI)

  - *Privacy Act 1988*
  - *Freedom of Information Act 1982*
  - *Income Tax Assessment Act 1936*
  - *Data-matching Program (Assistance and Tax) Act 1990*

  (Collection and use of PI)

  - *Census and Statistics Act 1905*
  - *Commonwealth Electoral Act 1918*

Snapshot of relevant legislation?

- **Commonwealth Legislation**

  (Disclosure of PI)

  - *Australian Passports Act 2005*
  - *Corporations Act 2001*
  - *Telecommunications Act 1997*
  - *Telecommunications (Interception and Access) Act 1979*
  - *Migration Act 1958*

Snapshot of relevant legislation?

- **NSW Legislation**
  - *Privacy and Personal Information Protection Act 1998*
  - *Health Records and Information Privacy Act 2002*
  - *Workplace Surveillance Act 2005*
  - *Surveillance Devices Act 2007*

- **Other States also have numerous pieces of legislation**

Bartier Perry

Snapshot of relevant legislation?

- **Conclusions of ALRC / Senate Enquiry**

  - Australia's Privacy Laws are multi-layered, fragmented and inconsistent

  - Inconsistency and fragmentation causes unjustified compliance burden and costs, impediments to information sharing and national initiatives ad confusion about who to approach to make a privacy complaint

Why the changes?

- **ALRC Report # 108 "For your information: Australian Privacy Law and Practice"**
  - 295 changes recommended by ALRC
  - First stage amendments implement 197 of them by:
    - introducing single set of privacy principles to apply to Commonwealth Agencies and private sector organisations (replace IPPs and NPPs)
    - introducing comprehensive credit reporting (objective consistency, simplicity and clarity
    - introducing new provisions for Privacy Codes;
    - clarifying functions and powers of Privacy Commissioner

Type of Legislation

- **Technology neutral**
- **Principles-based law**
  - High level principles to give flexibility
  - Flexibility allows handling of personal information to be tailored for diverse business needs and models and to diverse needs of clients
  - Plenty of open spaces

What are the Australia Privacy Principles?

Bartier Perry

1. Open and transparent management
2. Anonymity and pseudonymity
3. Collection of solicited
4. Dealing with unsolicited
5. Notification of the collection
6. Use and disclosure
7. Direct marketing
8. Cross border disclosure
9. Adoption, use or disclosure of government identifiers
10. Quality
11. Security
12. Access
13. Correction

Some of the requirements

- **APP 1 - Open and Transparent management**
  - More prescriptive requirements for privacy policies – policies must have
    - kinds of information collected;
    - how individual may complain about breach; and
    - whether organisation is likely to disclosure information overseas
  - APP 1.2 - ***Positive obligation for organisations to implement practices, procedures and systems that will ensure compliance***

Some of the requirements

- **APP 2 – Anonymity and pseudonymity**
  - Must have option to deal with entity anonymously or by using a pseudonym **unless**
    - Entity required or authorised by or under Australian law to deal with individuals who have identified themselves; or
    - it is impractical for entity to deal with individuals who have not identified themselves or who have used a pseudonym

Some of the requirements

- **APP 3 – Collection of solicited PI**
  - An organisation must not collect PI (other than sensitive information) unless it is ***reasonably necessary*** for one of its functions or activities
  - Intended to be interpreted objectively and in a practical sense
  - Reasonable person's, not entity's, perspective – which may mean that collection may not be reasonably necessary even if the entity cannot effectively pursue that function or activity without collecting the PI (NB guide gives a more practical interpretation)

Some of the requirements

- **APP 4 – Collection of unsolicited PI**
  - New principle (unsolicited not defined – solicit is)
  - Could the information have been collected under APP 3?
  - If yes, must be protected in the same manner as solicited PI
  - If not, must be destroyed or de-identified

Some of the requirements

- **APP 4 – Collection of unsolicited PI**
  - Examples of unsolicited PI
    - misdirected mail
    - correspondence to Ministers and Govt Depts from members of the community
    - a petition with names and addresses
    - an employment application on an individual's own initiative but not in response to an ad
    - Promotional flyer containing PI sent by an individual promoting a business or service
    - Additional PI provided that was not solicited

Some of the requirements

- **APP 5 – Notification of collection of PI**
  - essentially maintains the requirements of NPP 1 with the added requirements that notification is given:
    - APP privacy policy contains information about how to access and seek correction of PI and info about complaints process;
    - whether likely to disclose PI to overseas recipients and, if it is practical to specify, the countries in which those recipients are likely to be located; and
    - if PI collected from a third party, that the PI has been collected, and the circumstances of that collection

Some of the requirements

- **APP 6 – Use and disclosure**
  - Only be used or ***disclosed*** for the purpose it was collected (primary purpose) unless:
    - individual's consent provided; or
    - an exception applies – essentially the same exception under NPP 2 with the following additions:
      - assist to locate a missing person
      - for the establishment, exercise or defence of a legal or equitable claim;
      - for confidential alternative dispute resolution process.

Some of the requirements

- **APP 7 – Direct Marketing**
  - Now its own discrete provisions / no longer a "secondary purpose"
  - Prohibited except in certain circumstances
  - communicating directly with consumer to promote the sale of goods or services
  - Any form (mail, telephone, email or SMS)
  - Source of information must be recorded and disclosed, if requested.

Some of the requirements

- **APP 8.1 – Cross Border Disclosure**
  - **before** an entity ***discloses*** PI to a person that is not in Australia or an external territory; and
  - is not the entity or the individual,

  the entity must take such ***steps as are reasonable*** in the circumstances to ensure that the overseas recipient does not breach the APPs in relation to that information

  - Section 16C in certain circumstances a breach by an overseas recipient may be a breach by the entity

  - Designed to allow disclosure subject to protection

Some of the requirements

- **What does “disclosure” or “disclose” mean?**
  - Not defined in Act
  - The release of information from its effective control
  - Examples:
    - sharing of PI with another entity
    - publication of PI on the internet and it is accessible by other entities (even if not collected); and
    - PI sent by accident to the wrong person

Some of the requirements

- **APP 8.2 – exceptions to 8.1**
  - Alternative to taking reasonable steps, entity ***"reasonably believes"*** at least the equivalent protection under foreign law
    - need accessible mechanisms to enforce protections
  - Individual consents – (express or implied s 6(1))
  - Disclosure required by law

Some of the requirements

- **APP 9 – adoption, use or disclosure of Govt related identifiers**
  - An organisation must not adopt, use or disclose a Got related identifier of an individual as its own identifier of the individual unless exceptions apply.
  - Why? EM – Govt related identifiers are generally highly reliable for verification and identification of individuals – not to become universal identifiers
  - Exceptions include – *"the use or disclosure of the identifier is reasonably necessary for the organisations to verify the identify of the individual for the purposes of the organisation's activities or function."*

Some of the requirements

- **Part 4 – Integrity of personal information**

  APP 10 – quality of personal information

  - Take steps as are reasonable in the circumstances to ensure that personal information that the entity collects is accurate, up-to-date and complete.

  - If it uses that information, it must also be relevant

  APP 11 – security of personal information

  - Reasonable steps to protect from misuse, interference, loss, unauthorised access, modification or disclosure
  - Destroy or de-identify information if no longer needs the information for any purpose

Some of the requirements

- **Part 5 – Access to, and correction of, personal information**

APP 12 – Access

- If the entity holds personal information, the entity must on request by the individual, give access to the information. (reasonable charge for organisations)

- If it uses that information, it must also be relevant

APP 13 – correction of personal information

- Entity must take such steps (if any) as are reasonable in the circumstances to correct information to ensure that, having regard to the purposes for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

Change to definition of PI?

- **What is 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 material form or not

- **Bring in line with international standards and precedents (EM)**

Identity v Identification?

- **Distinction between identity and identification of an individual**

  - "Identity" – range of different identities defined by relation with others, position, status, actions, behaviours, characteristics, attitudes

  - "Identifying" focusing on those things that distinguish that individual from others (eg legal name, date of birth, location or address, driver's licence)

    - M Crompton, "Under The Gaze, Privacy Identity and New Technology" (Paper presented at International Association of Lawyers 75th Anniversary Congress Sydney, 28 October 2002).

How is an individual identified?

- **Identification**
  - Distinguishing individual from other members of a group – Name is not necessary – Physical/digital

- ***identified individual or reasonably identifiable***
  - ***Given technology these days, is all information held by agencies and organisations potentially information about an identifiable individual?***
  - **Test** – reasonably identifiable when it may be possible using available resources, the cost, the difficulty, practicality and likelihood of the person or entity doing so
  - **Must look at the context**

Bartier Perry

PI Test 1

Questions

1. CCTV system allows the operator to distinguish an individual based on physical characteristics but not name.

2. Information of web user built up over time, with intention of later linking it to a name and address.

3. Same as 2 but no intention of later linking the information to a name and address, merely to target user with marketing material.

PI Test 1

- **Answers**

1. Yes

2. Yes

3. Yes – *"In the context of the on-line world the information that identifies an individual is that which uniquely locates him in that world, by distinguishing him from others."*

UK Information Govt Information Commissioner Office Data Protection Act 1998 Legal Guidance (2001), 12

PI Test 2

- **Questions (Draft Guide)**

1. Holding of licence plate details.

2. Information that an unnamed person living in a particular area has a certain medical condition.

PI Test 2

- **Answers**

1. No in most cases, but would be personal information if the information is held by an agency responsible for car registrations

2. No in most cases, but would be personal information if it was provided to an individual with specific knowledge of those medical conditions and the suburbs where they live

Bartier Perry

Information Technology today

BIG DATA

- generally any data that is too big or is generated too fast for conventional systems, or is lacking well defined structure.
- Attributes - its volume, velocity and variety.
- Collection of large volumes of data of all types and variety in real time.
- collected from social networks, online websites, sensor readings from mobile devices, text, video and audio from traditional outlets, the utilisation of Big Data lies in the ability to ***“listen to what [it is] telling [the business] and then think about how to monetize that.”***

.

Information Technology today

The power of 1%

- One of the challenges of any business collecting information from various sources is to ensure that the information is accurate and reliable.
- The process therefore requires raw data to undergo a “cleaning” process.
- Often facilitated by organisations partnering with one another to exchange information which will allow the accuracy and reliability of information to be tested or verified.

.

Bartier Perry

Information Technology today

The power of 1%

- Beyond the benefits of exchanging information for cleaning or verification purposes, sharing customer information between financial service providers, retailers, and telecommunications businesses may lead to each provider better understanding the needs, wants, preferences and habits of its customers and producing very specific products, services and pricing.

Information Technology today

The power of 1%

- Whether information or data is exchanged as part of the cleaning/verification process or to allow for products and services to be better tailored to the customer's needs, wants, habits or preferences, the scope for data sharing arrangements by businesses has increased and may present a more economical and practical method of providing more innovative products, services and pricing for customers.

PI Test 3

Question

1. Ms X [16 yr school girl] buys products from retailer T. Retailer T is part of a larger group of companies, which form part of the C Group. Each group member is a separate entity and carries one a different business and sells a different range of products. Retailer T shares information with other C Group companies, and as a result is able to track purchases of Ms X. Analysis of her purchases with the C Group allows retailer T to determine that Ms X is most likely pregnant. Retailer T then starts directly marketing to her baby and maternity products. Is the collection of information about Ms X's purchases PI?

PI Test 3

Answer

1. Most likely. – It does not matter if name is not known, if retailer T can identify the customer by some distinguishing feature. In reality retailer T is mostly likely able to and wants to know the customers name.

Bartier Perry

Test 3

Question

1. One of things retailer T uses the information for is to allow it to tailor pricing to the customer to maximise profit. In its privacy policy, retailer T only says:

> *"We collect information for a number of reasons **including** to deliver products or services to you, to complete other transactions with you or on your behalf, to improve our service, to protect against fraud or theft and to provide offers that are of **greater interest or benefit to you**."*

Has retailer T complied with APP 1.4(c) - does it contain information about the purposes for which the entity collects, holds, uses and discloses personal information?

Test 3

Question

2. Has retailer T complied with AAP 3.5 ? -

> *An APP entity must collect personal information only by lawful and fair means [and not in an unreasonably intrusive way].*

EM says “The OAIC has interpreted “fair” to mean without intimidation or **deception**. The concept of fair would also extend to the obligation not to use means that are unreasonably intrusive.”

Test 3

Question

3. Retailer T includes in its privacy policy the following statement:

> *"Sometimes, we may add to your personal information additional information from external sources. This is mainly done to verify the accuracy of the information we have and, again, to personalise and improve our services."*

Does this additional statement affect compliance with APP 1.4(c) or AAP 3.5?

How easy is it to avoid collecting PI?

- **De-identification**

  - data or information is altered to remove or obscure personal information or Govt related identifiers – so the individual is no longer an identified individual or reasonable identifiable; and

  - risk of re-identification is minimised (which risk depends on the context and circumstances, and the nature of the information,

then not Personal Information.

How easy is it to avoid collecting PI?

- **De-identification**
  - How do you de-identify an individual in a digital world from his digital identification/characteristics?

Challenges by 12 March 2014

- Tailor privacy policy to meet new requirements
- Take such steps as are reasonable in the circumstances to implement **practices, procedures and systems** relating to functions and activities that ensure compliance
- Understand what is reasonable in the circumstances

For more information

Please contact:

Norman Donato

Executive Lawyer

02 8281 7863

ndonato@bartier.com.au