



# Professional Practice in Engineering Management

University of Sydney Faculty of  
Engineering & Information  
Technologies



# Practical Privacy Law

Michelle Rowland  
Senior Lawyer, Gilbert + Tobin  
BA(Hons), LLB, LLM

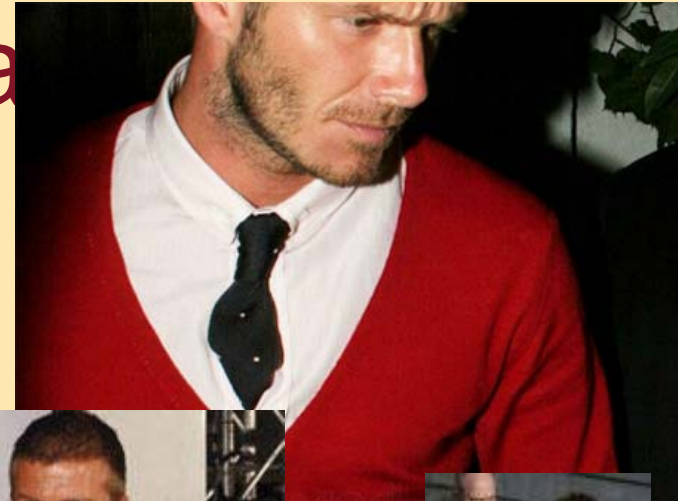


# Overview

- Where to start
- What to ask
- Refresher on the NPPs
- Some frequently asked questions
  - sale of business
  - offshoring/outsourcing
  - marketing
  - Commonwealth contractors
- Complaints/investigations/conciliations



# Privacy – cardigan





## Where to start – what privacy law applies?

- Private sector organisations
- Commonwealth agencies (public sector)
- State & Territory agencies (public sector)
- National Privacy Principles – contained in Privacy Act 1988, Sch 3 (NB exceptions apply)
- Information Privacy Principles – contained in Privacy Act, s14
- NSW, Victoria, Tasmania, Northern Territory all have enacted State privacy legislation; ACT agencies bound by Privacy Act 1988



## Where to start – what privacy law applies? (cont')

- Credit providers
- Carriers, carriage service providers
- Health information
- Part IIIA Privacy Act 1988 (also Credit Reporting Code of Conduct)
- Telecommunications Act 1997, Part 13
- Health records/privacy legislation in NSW, Vic, ACT



## Where to start – what privacy law applies? (cont')

- Also remember that there are a range of other “privacy related” laws, including:
  - State and Territory surveillance legislation (different in each jurisdiction) and listening devices legislation;
  - Marketing legislation – Spam Act 2003, Do Not Call Act 2007 (often overlaps with Privacy Act 1988)
  - Telecommunications (Interception and Access) Act 1979



# Applying the NPPs

- Today's focus will be on the private sector provisions in the Privacy Act – the National Privacy Principles (NPPs)
- 90%+ of privacy queries from G+T clients are NPP queries
- The NPPs regulate the collection, use, disclosure, storage and handling of “personal information” (s6)
- “Personal information” is information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion
- Special rules apply to “sensitive information”



## When is information “personal information”?

- Some practical tests for working out whether information is “personal information”:
  - If the information can easily be combined with other known information so that a person’s identity becomes apparent, the information should be regarded as personal information (ALRC)
  - Can a person be identified from data with “minimal additional research”? If yes – personal information (Senate Committee)



# Working through the issues ....

- If you receive a query from a private sector client about privacy – and you have established that:
  - the query relates to personal information; and
  - the NPPs are the relevant law ....
- you next need to think about relevant exceptions (to the definition of “organisation”) and exemptions (to acts and practices regulated under the NPPs)...



## Private sector privacy – are there any exceptions/exemptions?

- “Organisations” (defined in s6C) must comply with the NPPs in the Privacy Act
- An “organisation” includes an individual, a body corporate, a partnership, an unincorporated association, a trust ...
- Important exceptions to the definition of “organisation” – does not include a “small business operator”, a registered political party, a Commonwealth “agency”, or a



## Private sector privacy – are there any exceptions/exemptions? (cont’)

- “Small business” defined in s6D – annual turnover for the previous financial year was \$3m or less
- BUT a body corporate is not a small business if it is related to a body corporate that carries on a business that is not a small business (see s6D(9))
- NB – “annual turnover” - all income/revenues (s6DA)
- Also – s6D(4) specifies who is not a small business operator (health service providers, entities that disclose personal information for a benefit, service or advantage etc, contracted service providers to Cth)



# Small businesses?





## Exempt acts & practices

- Section 7(1)(ee) – a reference in the Privacy Act to an “act or practice” is a reference to “an act done, or a practice engaged in, by an organisation”
- Exempt acts or practices specified in s7B & s7C:
  - individuals acting in non-business capacity;
  - organisations acting under Cth Govt contracts (s95B regime applies)
  - acts/practices directly relating to a current/former employment relationship and an employee record



## Exempt acts & practices (cont')

- acts/practices by media organisations in the course of journalism (where journalism standards apply);
- organisations acting under a State government contract; and
- acts/practices of members of Parliament, a local government councillor in connection with elections/participation in the political process; contractors to political parties and volunteers also exempt



## Exempt acts & practices (cont')

- Employee records exemption is often referred to
- Important to note that the act or practice must directly relate to the current or former employment relationship and the employee record
- “Employee record” is defined in broad terms in s6 –a record of personal information relating to the employment of the employee
- Includes personal information about terms and conditions of employment and the employee’s performance or conduct (etc)



## Exempt acts & practices (cont')

- Common examples of where employee records exemption is relevant:
  - “we want to centralise our employee records database, so that employee records are stored in the US”
  - “we’re in negotiations to sell our business; can we put employee information in the due diligence data room? What about contractor information?”



## Exempt acts and practices (cont')

- Also, s13B provides that exchanges of personal information between related bodies corporate will not be an interference with the privacy of an individual
- The effect of s13B is that the collection of personal information by a body corporate from a related body corporate won't need to comply with NPP1; and the same applies to the relevant disclosure
- However, use of that personal information is regulated under NPP2. Also – remember that NPP9 applies



## To recap ...

- First ask – is the query about “personal information”?
- Then ask - what jurisdiction are we looking at?
- Next ask – are there any relevant exceptions or exemptions here (ie do any of the exceptions to the definition of “organisation” apply? are we talking about an exempt act or practice?)
- Once you’ve confirmed the answers to these questions, you then need to think about which NPPs raise compliance issues



# The NPPs – Collection – NPP1 and NPP10

- Collection must be necessary for the organisation's functions or activities (NPP1.1)
- Collection must be by lawful/fair means and not unreasonably intrusive (NPP1.2)
- Reasonable steps must be taken to make the individual aware who has collected their personal information, the purposes of collection, who it may be disclosed to, the individual's access rights, laws that required the collection to occur, and any consequences to the individual if it is not collected (NPP1.3)



# The NPPs – Collection – NPP1 and NPP10

- Personal information should be collected directly from the individual where reasonable/practicable to do so (NPP1.4)
- If indirect collection occurs, reasonable steps must be taken to make the individual aware of the matters in NPP1.3 (ie the collection notification provisions)
- Consent needed to collect sensitive information under NPP10 (ie information about a person's health, race/ethnic origin, political opinions/membership, religion, trade union/professional or trade association membership, sexual preferences, criminal record)



# The NPPs – Collection – NPP1 and NPP10

- Important points:
  - generally, an individual doesn't need to consent to collection (unless it is sensitive information)
  - however organisations should only collect what they need, and in practice, NPP1.3 and NPP1.5 can raise challenges. Need to make a judgement call about what amounts to reasonable steps
- See OFPC Information Sheet 18 (*“Taking reasonable steps to make individuals aware that personal information about them is being collected”*)



# The NPPs – Use & disclosure

## – NPP2

- Must be for primary purpose of collection; or
- for a secondary purpose (related to that primary purpose) that the individual would reasonably expect
- Otherwise - consent is generally needed
- Exceptions to this include:
  - use or disclosure required by or authorised under law;
  - disclosure to law enforcement agencies;
  - direct marketing (if impracticable to seek consent before the use for direct marketing purposes, and if marketing material contains opt out etc)



# Marketing

- NPP2 allows use of personal information for marketing if:
    - primary purpose of collection is marketing
    - marketing is a secondary purpose related to the primary purpose that is “reasonably expected”
    - the person consents; OR
    - the “direct marketing exception” applies
- NB Additional rules for electronic and telephone marketing under Spam Act and Do Not Call Register Act



# The NPPs – Accuracy & Security

- NPP3 – Accuracy - take reasonable steps to make sure that personal information that is collected, used or disclosed is accurate, complete and up to date
- NPP4 – Security – take reasonable steps to protect personal information from misuse, loss, unauthorised access modification or disclosure (NPP4.1)
- Also take reasonable steps to destroy or de-identify personal information if no longer needed for a purpose permitted under NPP4.2
- Many organisations don't comply with NPP4.2



# The NPPs – Openness & Access

## NPP5: Openness

- Privacy Policy – must make it available to anyone who asks (explaining what personal information is collected, why and how collected, and how it is used and disclosed)

## NPP6: Access and Correction

- Individuals have rights to seek access to and correction of personal information held about them
- Some exceptions apply (eg unreasonable impact on privacy of others; information would not be accessible under discovery processes, impact on health & safety)



# The NPPs – Identifiers & Anonymity

- NPP7 and NPP8 are rarely raised by are noted here for completeness
- Under NPP7, an organisation cannot use a Commonwealth government identifier (eg a tax file number or a social security number) as its own identifier for a person
- Note that there are special rules re TFNs
- Under NPP8, an individual has the right to remain anonymous where it is lawful and practicable for them to do so (eg if making a telephone inquiry)



# The NPPs – transborder data flows

- Under NPP9, an organisation can transfer personal information about an individual to someone overseas if:
  - the recipient is subject to a law which effectively upholds principles that are substantially similar to the NPPs; or
  - if the individual consents; or
  - the organisation has taken reasonable steps to ensure that the information transferred will not be held, used or disclosed by the recipient inconsistently with the NPPs
- There are some other grounds too ...



# The NPPs – transborder data flows

- Examples of countries which have privacy laws that reflect principles substantially similar to the NPPs:
  - New Zealand
  - Hong Kong
  - Japan
  - EEA/EU countries that have implemented the EU Directive (eg UK, France, Germany, Italy)
- USA and nations in SEast Asia, Middle East – need contractual protections in place (must be monitored)



## FAQs – 1. Sale of business

- Privacy issues often arise during a sale of business process
- Very useful guide – OFPC Information Sheet 16 (Application of key NPPs to due diligence and completion when buying and selling a business)
- This gives examples of what can be disclosed during due diligence processes, and upon completion (in relation to employee information and customer information)
- NPP1, NPP2, NPP4 and NPP10 are relevant



## FAQs – 1. Sale of business (cont')

- During due diligence process, OFPC's view is that:
  - vendor disclosures of employee information will fall within the employee records exception if directly related to employment relationship (but potential purchasers won't be covered by the exception)
  - ask whether aggregated info is sufficient
  - vendor disclosures of customer information will be related to the primary purpose of collection and reasonably be expected by the individual BUT steps should be taken to restrict use



## FAQs – 1. Sale of business (cont')

- Upon completion – personal information will be transferred if the sale is a sale of assets
  - re employees - OFPC considers that transfer of employee information would generally be directly related to the employment relationship
  - re customers - if purchaser will continue to provide the same goods or services as the vendor business disclosure would be consistent with the primary purpose of collection



## FAQs – 1. Sale of business (cont')

- otherwise, need to consider reasonable expectations of customers, and whether consent is needed to effect transfer
- consent may be needed if the purchaser organisation contemplates significant changes to the character or operations of the business
- Remember that purchaser/potential purchaser has obligations too
- Disclosure of executive salaries often an issue (eg informing employees prior to disclosure)



## FAQs – 2. Offshore transfers

- Example– Australian subsidiary’s parent company wants to centralise its employee records
- Should fall within the employee records exception
- s13B will also be relevant
- However, if the employee records database also contains personal information about contractors, NPP9 will need to be complied with



## FAQs – 3. Offshoring generally

- Organisation wants to certain functions to be carried out offshore by an external service provider
- NPP9 will apply to the transfer; and also NPP2 and NPP4 in particular (use and disclosure and security)
- OFPC's view is that customers should be made aware that their personal information will be handled offshore (eg in privacy policy or privacy notices)



## FAQs – 4. Marketing

- Have the Spam Act and the Do Not Call Register Act overtaken the Privacy Act where marketing is concerned?
- Note that there is some overlap – ie the Spam Act regulates the sending of commercial electronic purposes, and the Privacy Act may regulate the use of the relevant email address for that purpose (if the email address is personal information)
- The same can also apply under the Do



## FAQs – 5. Commonwealth Govt Contracts

- s95B requires contracted service providers to the Cth not to do an act or engage in a practice that would breach an IPP if done by an “agency”
- the standard clause also requires contractors to comply with those additional obligations under the NPPs that aren’t reflected in the IPPs
- See AGS model clause in Legal Briefing No 63 (*Outsourcing: Agency Obligations*)



# Privacy Regulators





# Complaints and investigations

- Under s36, individuals can complain to Privacy Commissioner about an act or practice that may be an interference with their privacy
- Privacy Commissioner investigates complaints under s40
- Privacy Commissioner won't investigate complaints if s41 applies – eg complaint is made more than 12 months after the individual became aware of the act or practice; or is frivolous or vexatious; or if the complaint has been adequately dealt with under another law (etc)
- Broad powers of investigation (re production of docs etc)



## Complaints and investigations (cont')

- OFPC adopts a “conciliation approach” in practice
- However, if no conciliation, Privacy Commissioner can make determinations under s52
- s52 determinations can include a declaration that the organisation has engaged in conduct that interferes with a person’s privacy, and should not repeat or continue such conduct; that action should be taken to redress any loss or damage suffered; that the complainant is entitled to a specified amount of compensation
- Enforceable in Federal Court/Federal Magistrates Court
- Bad publicity may also follow



## Compensation and financial settlements?

- OFPC has not made public much information about how much compensation is adequate
- Will depend on what the impact of the breach was (eg did a mistaken disclosure of personal information result in an individual's estranged spouse tracking them down? did it lead to someone not getting a job they'd applied for? or was the impact more minor?)
- In our experience - \$2,000 to \$5,000 (depending on what occurred); confidential settlements