



# Privacy in AU and NZ for NFPs

*Connecting Up* 

# Course Overview

- Who is covered?
- What is 'personal information'?
- Privacy Notices
- Collection
- Consent
- Marketing & privacy laws
- Spam laws
- Using cloud service providers
- Data breach notification obligations





# Presenter

---

- Dr Jodie Siganto CISSP CIPM CIPPE
  - Privacy and Information Security Lawyer and Consultant
  - Trainer
  - Researcher
- What we do:
  - Privacy compliance reviews
  - Develop privacy management programs
  - Assist when responding to data breaches
  - Privacy impact assessments
  - Security reviews
  - Privacy and security awareness training

# Introduction & Background

## Clarifying Some Misconceptions

- **FICTION:** Privacy Act protects you from reputational harm or embarrassment

*FACT: Privacy Act covers the concealment and protection of your personal information*

- **FICTION:** Privacy = Secrecy (only applies to secret info)

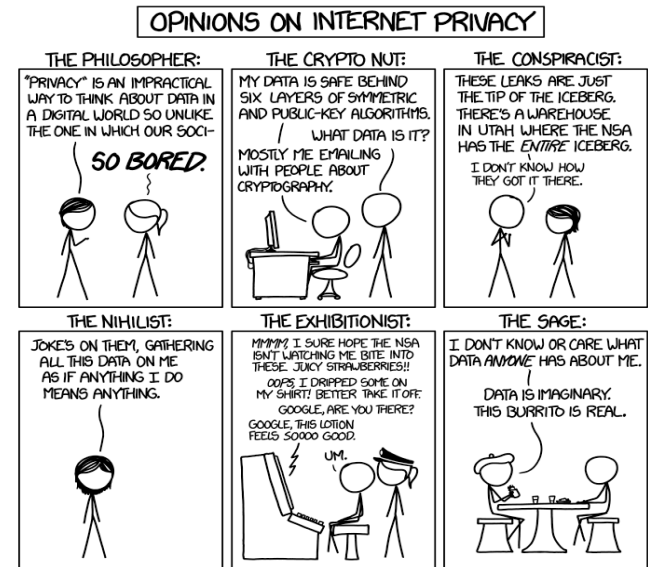
- *FACT: Privacy Act covers personal information that is publicly available*

- **FICTION:** Only applies to information you collect

*FACT: Covers information that you “create” from logs, cookies, data analytics etc. – not just the information that someone gives you*

# Social Attitudes to Privacy

- OAIC Community Attitudes to Privacy 2013:
  - 48% of Australians believe that online services, including social media, now pose the greatest privacy risk
  - 96% expect to be informed if their information is lost
  - 95% expect to be informed about how their info is handled on a daily basis
- Things that people are concerned about:
  - Loss of control over data
  - Transparency – what are organisations going to do with data
  - Understanding the different purposes and benefits of data sharing
  - Security – how does that work
  - Rights to access, delete and portability of personal information



# Privacy Laws - Who is Covered?

---

You probably are covered ...



## Territorial Application of Privacy Laws

- To be subject to Privacy Act of Australia or NZ, must *be carrying on business* in that jurisdiction
- Is targeting donors in the country sufficient?
- Is having an accessible website sufficient?
- Ashley Madison:
  - “Although ALM does not have a physical presence in Australia, it conducts marketing in Australia, targets its services at Australian residents, and collects information from people in Australia. ALM has advertised in Australia, and the Ashley Madison website at the time of the breach had pages targeted specifically at Australian users. For this reason, it carries on business in Australia.”
- European privacy laws have broad extra-territorial application



## Who is Covered?

### Australia:

- Commonwealth government agencies
- An individual (including a sole trader)
- Other legal entities e.g. body corporate, partnership, **any other unincorporated association**, or trust

### New Zealand:

**'agencies' -> any business or organisation, whether it's in the public sector or private sector, including:**

- Government departments
- Companies
- Small businesses
- Social clubs
- Other types of organisations.

# Who is Covered? - Some Exemptions

## Australia

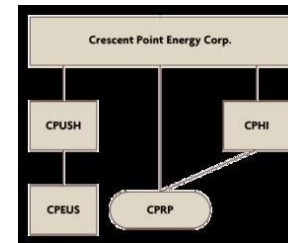
- Personal information collected for **personal, family or household use**
- Political parties and journalists
- Small businesses - < \$3 million p.a. (but “carve ins”)
- State government agencies (and contracted service providers to State government agencies)

## New Zealand

- Courts and tribunals when they are doing their judicial tasks
- News media when they are gathering and reporting news
- Members of Parliament (MPs) when they’re acting in an official capacity.

# Sharing information within the group?

- Organisations which belong to the same corporate group can exchange information with each other (test = shared controlling interest)
- Must still comply with other principles :  
Example: If obtain consent on collection to use of PI for purpose of marketing - related company can use it for the same marketing purpose e.g. marketing of their products & services *U v Telecommunications Company* [2009] PrivCmrA 24
- If transfer to overseas related body corporate - Still need to comply with APP 8 (cross border data flows)



# What happens if someone goes rogue?

- Liability for employees:

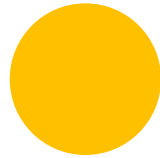
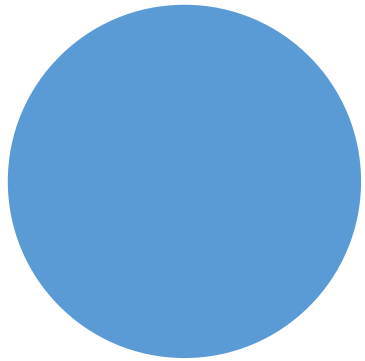
“an act done or practice engaged in by, or information disclosed to, a person employed by, or in the service of, an [entity] ... in the performance of the duties of the person’s employment shall be treated as having been done or engaged in by, or disclosed to [the entity].” Section 8(1)(a):

- Will be liable for acts of employees even if not aware of them e.g. *P v Electrical Goods Retailer* [2006] PrivCmrA 15
- But entity’s general privacy practices will be taken into account e.g. One off human error vs systemic failure *Telstra Mail Out Own Motion Investigation* (2011)



**Rogue Employee Costs  
Greenpeace \$5.2M**

Jun 17, 2014 12:08 AM CDT



What is Personal |  
Information?

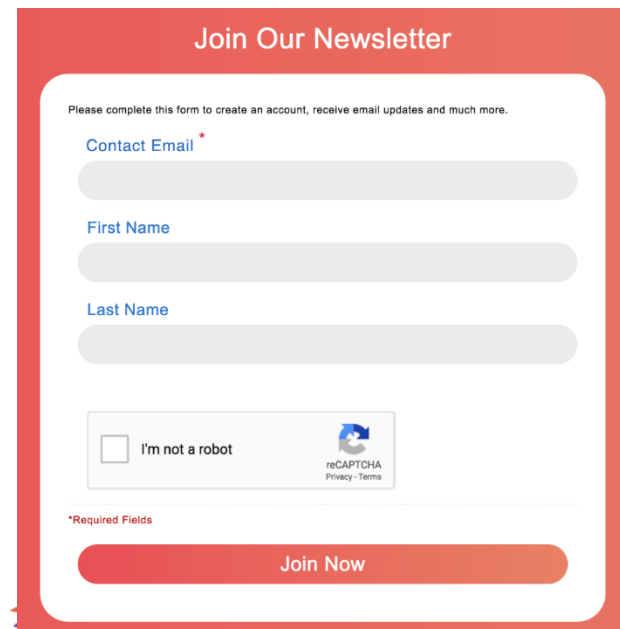
# What is “Personal Information”

Australia: “... Information or an opinion about an identified individual, or an individual who is *reasonably identifiable*”

New Zealand: “... Information about an identifiable individual”

## Examples:

- Name of clients, donors, contacts in other services providers
- Contact details
- Photos, CCTV, videos
- Bank account details & financial info
- Details of interactions with your agency




Join Our Newsletter

Please complete this form to create an account, receive email updates and much more.

Contact Email \*

First Name

Last Name

☐ I'm not a robot  reCAPTCHA  
Privacy - Terms

\*Required Fields

Join Now

# Australia ONLY - Sensitive Information

*Personal information* that is also about an individual's:

- Racial or ethnic origins
- Political opinions or membership of a political association
- Religious beliefs or affiliations
- Membership of a professional or trade association or union
- Sexual preferences or practices
- Criminal record

Health information

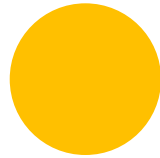
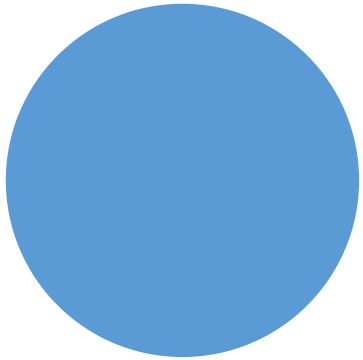
Genetic information

MUST NOT collect **sensitive information** unless the individual provides **consent**  
(discussed next)

# NZ Only - Health Information Privacy Code

- New Zealand's Privacy Act does not specifically regulate 'sensitive data'
- Health information is subject to specific protection through the *Health Information Privacy Code (HIPC)*
  - *the HIPC notes that agencies may need to give a more detailed explanation as to the intended use of information when particularly intimate or sensitive information is sought, or where it plans to use the information in an unexpected way.*





Privacy Policies



....

# Publish Your Privacy Policy

Privacy policies must generally describe the following:

- what types of personal information you collect and hold;
- how you collect that personal information (e.g. - directly from individuals through a form)
- how your business uses that information (the purposes you require it for);
- whether and when you disclose that personal information to any third parties;
- whether the entity is likely to disclose PI to overseas recipients
- how an individual may access their personal information or seek correction of it
- how an individual may contact your organisation

Resources:

- [Guide for drafting Australian privacy policies](#)
- [Guide for drafting New Zealand privacy policies](#)
- Plenty of templates and tools online...



# Think of your stakeholders' expectations

## Stick to what you commit to in your policy ...

- A guiding principle that will assist with privacy compliance is to stick to what your customers would *expect*
  - **How would our stakeholders expect us to deal with their information?**
  - **How would I expect my information to be dealt with if I were a donor or volunteer?**
- For example, if you run a NFP that collects health information, most individuals wouldn't expect you to on-sell their personal information to a personal injury law firm, and indeed might be quite upset if you do.
- By considering these simple questions, you are much more likely to remain compliant with Privacy Laws in your everyday dealings.

Permitted  
collection of  
personal  
information?

# Collecting Personal Information

An entity or agency can collect PI only if it is *necessary for one or more of the entity's functions or activities*

When would the collection of personal information be reasonably necessary?

Bank  
account  
details for  
processing  
monthly  
donations

Email  
address for  
the purpose  
of sending  
email  
receipts

Name and  
contact  
details of  
volunteers

Email  
addresses  
for the  
purpose of  
sending out  
NFP  
newsletter

# ‘Reasonably Necessary’

- APP Guidelines: Examples of collection of data not reasonably necessary:

Marital status  
for banking  
application

Medical  
practitioner  
taking photo for  
patient's file  
when not  
necessary to  
provide a  
health service

Collecting all  
info on driver's  
licence when  
only need to  
establish that  
person is > 18  
years old

Collecting info  
in case it may  
be needed in  
the future

Collecting info  
on behalf of  
another  
organisation

# AU Only - Collecting Sensitive Information

## Recap - What is Sensitive Information?

- Health or Genetic Information
- Racial or ethnic origins
- Political opinions or membership of a political association
- Religious beliefs or affiliations
- Membership of a professional or trade association or union
- Sexual preferences or practices
- Criminal record

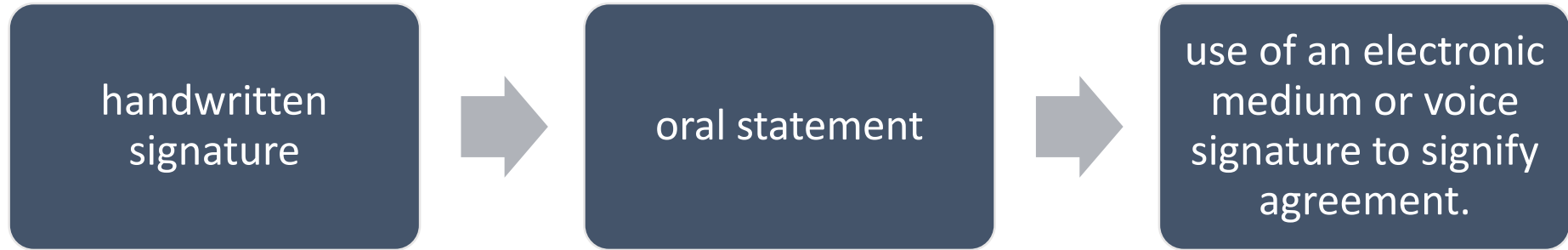
MUST NOT collect **sensitive information** unless:

1. The individual **consents**; AND
2. The information is **reasonably necessary** for your organisation's activities.

OR

Non-profit organisation and info relates solely to your members or individuals you has contact with

# Consent



Should generally seek **express consent** from an individual before handling the individual's **sensitive information**, given the greater privacy impact this could have



# Notice of Collection

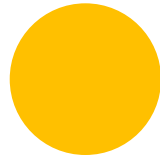
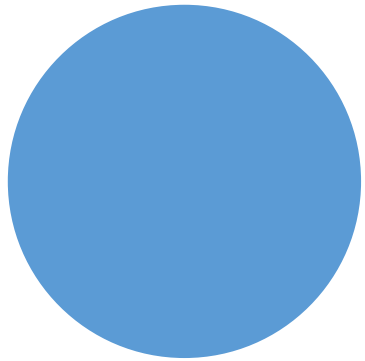
When collecting Personal Information we have an obligation to **notify the person** or **make them aware** that we are collecting their personal information.

*Applies to:*

- all personal information 'collected' about an individual, either **directly from the individual** or from a **third party**
- **solicited and unsolicited personal information** that is not destroyed or de-identified by the APP entity.

## Examples of Notifying and Making Aware:

1. Prominently displaying a collection notice on a form or website
2. Explaining full disclosure at the beginning of a phone call



Allowable use of  
personal information?

# Use or Disclosure of PI

Can only use or disclose PI **for the purpose for which it was collected.**

## Australia

“If an organisation collects personal information about an individual for a particular purpose (the primary purpose), it must not use or disclose the information for another purpose (the secondary purpose).”

## New Zealand

“Personal information that was obtained in connection with one purpose shall not [be used]... for any other purpose”

# Use and Disclosure

## Use

Examples of “use” include:

- Accessing and reading the PI or Searching records for the PI
- Making a decision based on the PI
- Passing the PI from one part of the entity to another

## Disclosure of Private Information

occurs when  
It becomes  
accessible or  
visible to  
others  
outside the  
entity

Examples of “disclosure” include:

- shares a copy of personal information with another entity or individual
- discloses personal information to themselves, but in their capacity as a different entity
- publishes personal information whether intentionally or not and it is accessible to another entity or individual
- accidentally provides personal information to an unintended recipient
- displays a computer screen so that personal information can be read by another entity or individual, e.g. at reception counter or in an office

# Use for secondary purpose

Can't use or disclose PI for secondary purpose **unless**:

Australia	New Zealand
<ol style="list-style-type: none"><li>1. Individual has <b>consented</b> to secondary use</li><li>2. Would reasonably expect use or disclosure for secondary purpose and the secondary purpose is:<ul style="list-style-type: none"><li>• <b>Directly related</b> to the primary purpose – for Sensitive Info</li><li>• <b>Related</b> to the primary purpose – if not Sensitive Info</li></ul></li><li>3. Required or authorised by or under an Australian law or a court/tribunal order</li><li>4. Prevent a serious threat to any individual's life, health or safety, or to public health or safety</li></ol>	<ol style="list-style-type: none"><li>1. You have the <b>authorisation</b> of the individual concerned</li><li>2. That the purpose for which the information is used <b>is directly related</b> to the purpose in connection with which the information was obtained; or</li><li>3. It's necessary to uphold or enforce the law.</li><li>4. Prevent a serious threat to any individual's life, health or safety, or to public health or safety</li></ol>

AU Guidance: [Here](#)

NZ Guidance: [Here](#)

What about  
using personal  
information for  
marketing?

## AU: Direct Marketing (APP7)

If entity collected info directly - can't use or disclose PI for purpose of direct marketing unless within exceptions:

The individual has a reasonable expectation that their personal information will be used for this purpose



Must provide simple means to 'opt-out', and the individual has not made such a request

## AU: Direct Marketing (APP7)

If entity collected info from third party or there is no reasonable expectation that info will be used for direct marketing - can't use or disclose PI for purpose of direct marketing unless within exceptions:

Must include a statement telling the individual that he or she may request to no longer receive direct marketing



Must provide simple means to 'opt-out', and the individual has not made such a request



# Anti-spam Laws

# Anti-Spam Laws

## Coverage

- Covers the sending of messages of a commercial nature by email, SMS instant message, or MMS

## Which Laws?

- Australia
  - *Spam Act 2003* (Spam Act)
  - *Do Not Call Register Act 2006* (DNCR Act)
- New Zealand
  - *Unsolicited Electronic Messages Act 2007*



## Anti-Spam Laws - Charities Exemption

### Australia

- Registered charities are exempt
- Must still include accurate sender identification in all emails, including the sender's contact information

### New Zealand

- No charities exemption
- However, Act applies only when 'marketing or promoting goods or services'
- If a not-for-profit does not market/promote goods or services (e.g. donations only), then the *Unsolicited Electronic Messages Act 2007* may not apply

# Anti-Spam Laws - Practical Compliance Steps

## Step 1 - Consent

- Express Consent - *Direct indication from the person you wish to contact that it is okay to send the message.*
- Inferred Consent - *Due to the person's conduct and your relationship with the person concerned, there is a **reasonable expectation that messages will be sent.***

## Step 2 - Identify Yourself

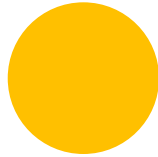
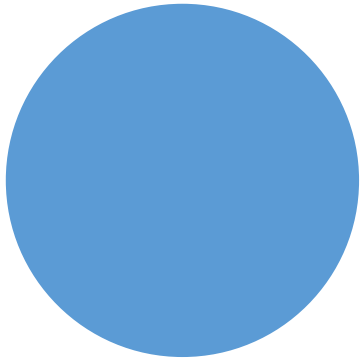
- Provide accurate sender identification including the sender's contact information

## Step 3 - Provide an Unsubscribe Button/Mechanism

- Messages must contain a low (or no cost) way for the recipient to stop getting messages (to 'opt out' or unsubscribe)

### Useful Guidance:

- AU: [ACMA - Spam Obligations](#)
- NZ: [DIA - Three Steps to Ensure You're Not Spamming](#)



Using cloud service  
providers



# Lots of issues with cloud service providers (CSPs) ...

- Is it appropriate to share the proposed data with the CSP?
  - Allowable use?
- Have you done due diligence on the CSP?
  - Financials;
  - Cultural fit;
  - Other clients.
- Have security issues been considered e.g.:
  - Controls used by the CSP;
  - Response to data breach;
  - Location and staffing.
- Have contractual issues been covered e.g.
  - Limiting right to access or use personal information;
  - Supporting individual access rights;
  - Return of data at end of contract.



# AU ONLY: Cross Border Disclosure [APP 8]

- There are restrictions on sending personal information out of Australia.
- May apply to using an off-shore cloud service provider e.g. Salesforce, SurveyMonkey

Before disclose to overseas recipient must “take such steps as are reasonable in the circumstances” to ensure the overseas organisation doesn’t breach the APPs \*

\*There are exceptions ...

# NZ ONLY: Cross Border Disclosure

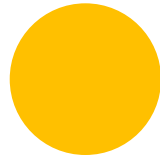
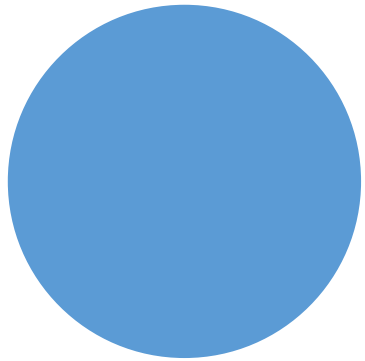
- Subject to compliance with the Information Privacy Principles, personal information may be transferred to a third country without restriction.
- For the purposes of Privacy Principles 5 (Storage), 8 (Accuracy), 9 (Retention), 10 (Limits on use) and 11 (Limits on disclosure), information transferred out of New Zealand is still considered to be held by the agency
- However, both the Privacy Act and the HIPC will continue to apply to personal information and health information even when it is transferred out of New Zealand.



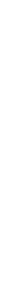
# Practical Exercise

**Which of the following might involve the disclosure of PI to an overseas recipient:**

1. Making PI available via a website which could be accessed from overseas e.g. Photos included in on-line newsletter
2. Sharing donor details via Dropbox
3. Saving advertiser list in Google documents
4. Engaging an overseas call centre to run a promotional campaign directed at existing clients (and sharing client list)
5. Using web survey tools e.g. Survey Monkey to collect PI
6. Collecting PI via a Facebook page
7. Using Office365 for your corporate email



# Data Security & Breach Notification Obligations



# APP 11

## Data Security Principle

- PI must take *such steps as are reasonable in the circumstances* to protect the information:
  - From misuse, *interference* and loss; and
  - From unauthorised access, modification or disclosure

- If entity no longer needs PI for any purpose for which the information may be used or disclosed ... Must take such steps are reasonable in the circumstances to *destroy the information or to ensure that the information is de-identified.*

## Eligible Data Breach - Australia

- Trigger for notification: “**Eligible data breach**”
- 2 components to an ‘eligible data breach’:
  - **Breach**: Unauthorised access, disclosure or loss of PI [e.g. hack, unauthorised posting on the internet, accidental emailing] OR the information lost in circumstances where unauthorised access or disclosure likely to occur [e.g. lost laptop]; AND
  - **Harm**: A reasonable person would conclude that, because of the access, disclosure or loss, there is a **likely risk of serious harm** to any of the individuals to whom the information relates

# Remedial Action Exception

Won't be an eligible data breach if you:

- Take action before the access or disclosure or loss results in serious harm; AND
- That action, in the opinion of a reasonable person, would result in there being no serious harm to any of the individuals

Example:

- Lost laptop is remotely wiped
- Take down info and ensure all cached copies removed

# Notification

- Notify **as soon as practicable** once aware there are reasonable grounds to believe there has been eligible data breach
- Notice of breach must contain:
  - Identity and contact details of entity
  - Description of breach
  - Kinds of information concerned
  - Recommended steps for affected persons to take in response to the breach

## Who is notified?

- If practicable - each individual to whom the compromised information relates
- If practicable – those individuals considered to be ‘at risk’ from the breach
- If neither of those are practicable – publish on website & take other reasonable steps to notify

# New Zealand and Data Breach Notification

- Currently no legal obligation to notify individuals of data breaches.
- Privacy Commissioner has issued guidelines to assist agencies respond to data breaches [here](#).
- Lists **four key steps**:
  - Contain the breach and make a first assessment
  - Evaluate the risks
  - Notify affected people if necessary
  - Prevent a repeat
- Encourages voluntary notification to individuals and Privacy Commissioner, where:
  - You're sure that the breach has compromised their information; **AND**
  - Data breach creates a risk of harm to a person, depending on whether:
    - there's a risk of identity theft or fraud
    - there's there a risk of physical harm
    - there's a risk of humiliation, loss of dignity, or damage to the person's reputation or relationships
    - you have any legal or contractual obligations

# New Zealand and Data Breach Notification

- Privacy Amendment Bill is expected to be passed in 2019, which will introduce mandatory data breach reporting.
- If introduced:
  - Notifiable if the “**privacy breach is likely to cause serious harm** to affected individuals”
  - Must notify Privacy Commissioner and affected individuals
  - Notify “**as soon as practicable** after becoming aware that a notifiable privacy breach has occurred”
  - Notify Commissioner of:
    - Number of affected individuals
    - Person in possession of breached PI (if known)
    - Steps taken to respond & proposed steps
    - Contact details
  - Notify individuals of:
    - Description of the breach
    - Steps taken to respond & proposed steps
    - Steps affected individuals should take
    - Commissioner notified and right to complain
    - Contact details



# CONCLUSION AND SUMMARY

# Similarities between AU and NZ Privacy Laws

Issue	Summary
Territorial Application of Laws	<i>Must be <u>carrying on business</u> in that jurisdiction</i>
Coverage - Personal Information	<i>Information about an identified or reasonably <u>identifiable individual</u></i>
Privacy Policy Required	<i>What personal information collected; how collected, used and disclosed; how an individual may access or seek correction; how an individual may contact you, etc.</i>
When Collection of Personal Information Permitted	<i>Collect PI only if it is <u>necessary for one or more of the entity's functions or activities</u></i>  <i>Provide notice of personal information collection</i>
When Use or Disclosure of Personal Information Permitted	<i>Can only <u>use or disclose PI for the purpose for which it was collected, unless:</u></i> <ul style="list-style-type: none"><li>• <i>Person provides consent</i></li><li>• <i>The second purpose is directly related to the original purpose for which the information was collected.</i></li></ul>

# Similarities between AU and NZ Privacy Laws

Issue	Summary
Anti-Spam Laws	<p><i>Permitted to send commercial emails where:</i></p> <ol style="list-style-type: none"><li><i>1. Consent has been obtained (express or inferred)</i></li><li><i>2. You have identified yourself</i></li><li><i>3. There is a functional unsubscribe mechanism</i></li></ol> <p>(Charities exempt in AU)</p>

# Differences between AU and NZ Privacy Laws

Issue	Summary
Coverage - Entities	<p><b>Both</b> apply to Not for Profits (unincorporated associations and social clubs)</p> <p><b>Australia:</b></p> <ul style="list-style-type: none"><li>• State governments and <u>State government contractors</u> covered by <u>State privacy laws</u></li><li>• Small businesses with <u>less than \$3m p/a turnover exempt</u></li></ul>
Sensitive Information	<p><b>Australia Only</b> (information about health, race, political opinions, religion, sexual preference etc.)</p> <p>Must not collect <b>sensitive information</b> unless the individual provides <b>consent (unless NFP and part of providing service)</b></p>
Marketing Laws	<p><b>Australia Only</b></p> <p>Can't use or disclose PI for the purpose of direct marketing unless:</p> <ul style="list-style-type: none"><li>• <b>Collected Directly</b> - Within the <u>individual's reasonable expectations</u></li><li>• <b>Otherwise</b> - With the <u>consent of the individual</u></li></ul> <p>Must provide means to <b>unsubscribe</b></p>

# Differences between AU and NZ Privacy Laws

Issue	Summary
International Transfers of PI	<p><b>Australia:</b></p> <ul style="list-style-type: none"><li>• Must take ‘reasonable steps’ to ensure the overseas organisation doesn’t breach the APPs</li></ul> <p><b>New Zealand:</b></p> <ul style="list-style-type: none"><li>• For the purposes of Privacy Principles 5 (Storage), 8 (Accuracy), 9 (Retention), 10 (Limits on use) and 11 (Limits on disclosure), information transferred out of New Zealand is still considered to be held by the agency</li></ul>
Data Breach Notification	<p><b>Australia:</b></p> <ul style="list-style-type: none"><li>• Mandatory to notify of data breaches that pose risk of “serious harm” to affected individuals</li></ul> <p><b>New Zealand:</b></p> <ul style="list-style-type: none"><li>• Not mandatory to notify individuals affected by a data breach</li><li>• But watch this space in 2019...</li></ul>

## Questions

**Jodie Siganto**

Jodie.siganto@ringrosesiganto.com.au

P: 1300 41 20 50

M: 0408 275 733

[www.ringrosesiganto.com.au](http://www.ringrosesiganto.com.au)