

Privacy Law Overview

Communications Essentials: Managing Service Provider Risks Under The New Privacy Laws

Communications Alliance Forum 16 April 2014

Patrick Fair
Partner
Baker & McKenzie

- Privacy fundamentals
- Overview of the new regime
- Focus on key provisions
- Credit Provider rules
- Questions and discussion

Overview

Privacy Law Framework

Regulates the handling of “Personal Information” by an “APP entity”


An “APP entity” can be an “agency” or an “organization”

Administered by the Office of the Australian Information Commissioner (**OAIC**)

Minimum standard is set out in 13 Australian Privacy Principles (**APPs**)

What is “Personal Information”?

- “... means information or an opinion about an **identified** individual, or an individual who is **reasonably identifiable**:
 - a) whether the information or opinion is true or not; and
 - b) whether the information or opinion is recorded in a material form or not.

 There is **no** requirement that the personal information be confidential information

Exemptions and special rules

Specific rules:

- for credit reporting
- sensitive information (includes biometric information)

Exemptions apply for:

- personal, family or household affairs
- small business
- political parties
- journalism
- “employee record”

Overview of New Regime

The new regime

New regime:

- in force from **12 March 2014**
- consolidated Australian Privacy Principles (APPs) (Schedule 1)
- new provisions on credit reporting (Schedule 2) and privacy codes (Schedule 3)
- new enforcement powers (Schedule 4)

The APPs

- Divided into 5 Parts (openness and transparency, collection, handling, integrity, access and correction)
- Key new requirements:
 - privacy policies
 - complaints handling
 - collection statements
 - unsolicited personal information
 - direct marketing
 - cross-border disclosures



APP 2: Anonymity and pseudonymity

- Individuals **must** have an option to use a pseudonym / not to identify themselves when dealing with an APP entity in relation to a particular matter unless:
 - identification required or authorized by law / court order
 - impracticable
- Not a new requirement, but APP2 is broader
- Not sufficient that it is desirable to identify the individual

APP 3: Collection of personal information

Distinction: non-sensitive v sensitive personal information

Non-sensitive

- for organizations must be **reasonably** necessary for one or more of the APP entity's functions or activities
- for agencies, must be **directly related to** one or more of the agency's functions or activities

Sensitive

- additional requirement of consent OR
- one of the exceptions applies

APP 3: New terms

- “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 organization:
 - relates to activities of the organization
 - relates to members or persons with regular contact

APP 3 & 4: Collection of personal information

Distinction: solicited v unsolicited

APP 3: solicited personal information

- Collection must be by fair and lawful means
- Only from the individual unless:
 - unreasonable or impracticable to do so
 - for agencies, can also collect from others if the individual consents **or** required/authorized by law/court order

APP 4: unsolicited personal information

- Assess: could you have collected the info under APP 3?
 - if no, must destroy the PI
 - if yes, APPs apply as if the PI was solicited

APP 6: Restrictions on use and 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 and directly related (sensitive information)
- reasonably expected and related (non-sensitive information)
- permitted general situation
- permitted health situation
- others

APP 6.3: exception for biometric information / templates sent to enforcement bodies

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 and unauthorized access etc.) and destruction/de-identification of PI if no longer needed* **more extensive**

APP 12: giving individuals access to PI

APP 13: correction of PI

Enforcement

Commissioner's powers:

- guidelines
 - vary registered APP Codes
 - investigations following complaints or on own initiative
 - mandatory orders
 - declaration of entitlement to compensation
 - prosecution in Federal Court / Fed. Magistrates Court
- monetary penalties of up to:
- \$340,000 (non-corporate entities / individuals)
 - \$1.7million (corporations)

Focus on Key Provisions

APP 1: Open and transparent management

- Reasonable steps to implement practices, procedures and systems to ensure compliance
 - Privacy by design
 - New approach to privacy compliance
 - Embed privacy protections in the design of information handling practices
- Clearly expressed privacy policy
- Reasonable steps to make policy available free of charge in an appropriate way

APP 1: Privacy by design

Leadership

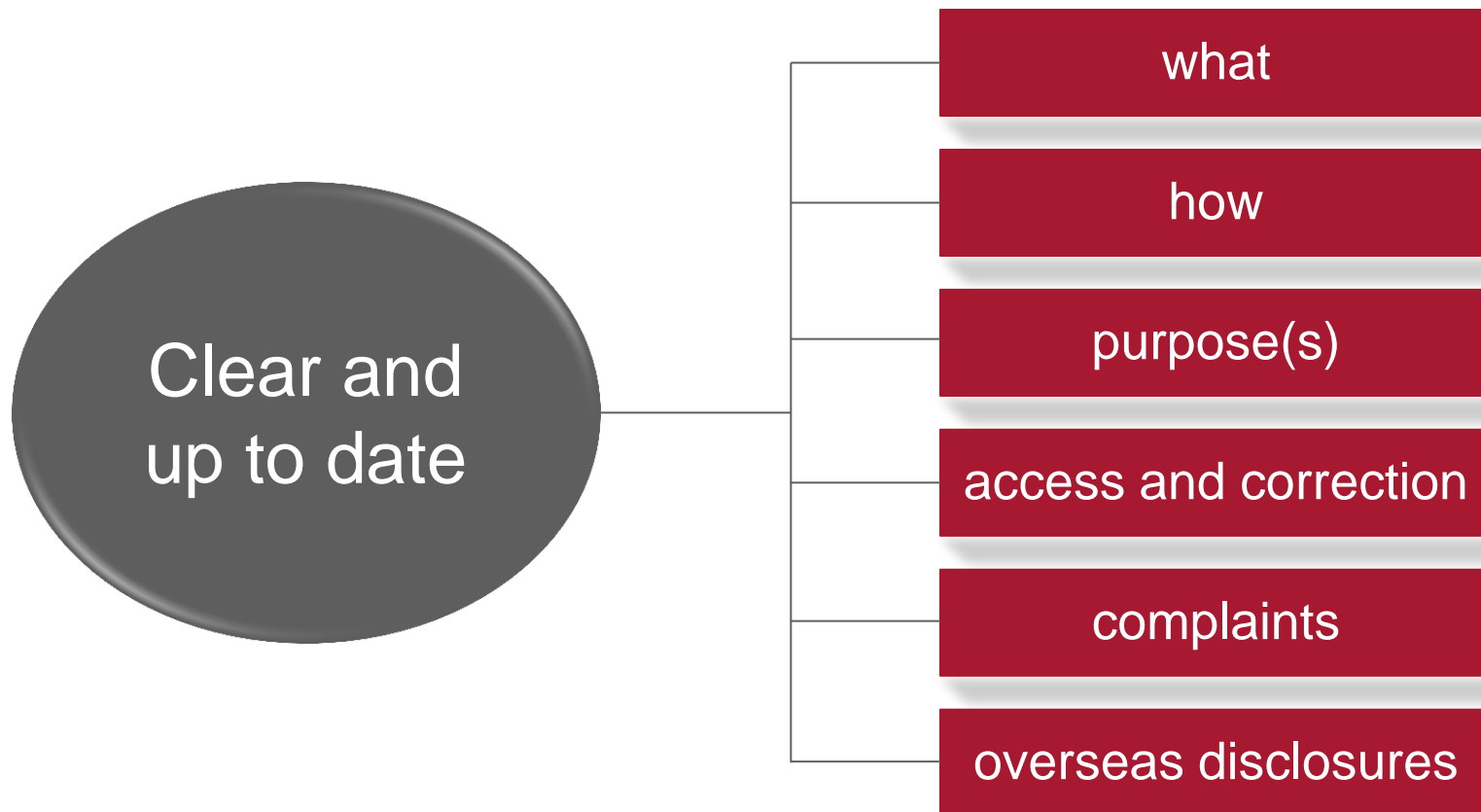
Risk
Assessment

Standards
and Controls

Training and
Communication

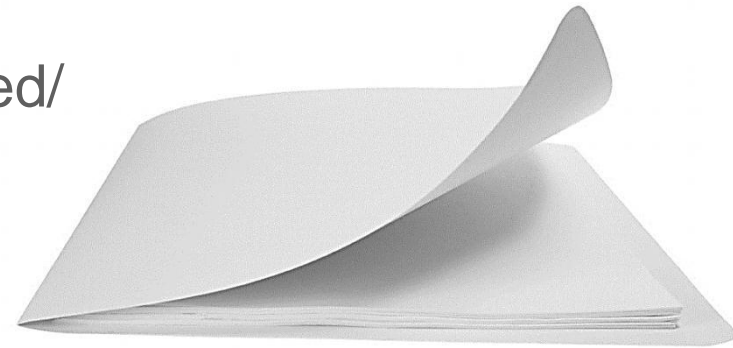
Monitoring, Audit
and Response

APP 1: Privacy Policy



APP 5: Collection notification obligation

- Identity and contact details of APP entity
- Not collected from data subject or not aware - fact and circumstances of collection
- Purpose
- Main consequences if information not collected
- Parties to which usually disclosed
- If applicable, that collection authorized/required by law or court order
- Policy describes access, correction and complaint mechanisms
- Disclosure overseas and where disclosure likely



APP 7: Direct marketing

Spam/DNR

- Not applicable if apply
- But only to extent apply
- Use or disclosure prior to sending/calling

APP 7.2

- PI collected from individual AND
- Reasonable expectation will be used for DM
- Must provide simple opt out
- Individual not opted out

APP 7.3

- PI not collected from individual OR
- no reasonable expectation that PI used for DM
- Consent required
- Prominent opt out
- Individual not opted out

APP 7.4

- Sensitive Information always requires consent

APP 8: Cross-border disclosure

APP 8.1:

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 strictly **liable for acts of overseas recipients** where there is disclosure!



Exceptions:

- at least substantially similar protection overseas
- warning and consent
- other exceptions (similar to APP3 / 6.2)

Background

Availability of services from low cost countries via the internet or dedicated networks

Services may be purchased directly by the enterprise or delivered by third parties

Local services may be provided wholly or partly from overseas

“follow the sun” support moves
2/3/4 times a day

The new privacy law regulates
“disclosure” not “transfer”



How might disclosure take place?


The nature of the data access provided offshore varies widely:

- storage “in the cloud” automatic back up vs. integrated
- processing “in the cloud”
- access to data via “business process outsourcing”
- provision of data for billing or fulfilment tasks
- locally based systems may be supported of shore:
 - first level support
 - second and third level support
- hardware support: systems administrator access




What might be reasonable steps?

Is the obligation to ensure that the recipient “does not breach” the APPs different from an obligation that it will fully comply with APPs?



Have regard to the full context: nature of information, relationship with recipient, risk of harm, existing technical and operational safeguards, practicality of steps



Possible solutions: contract terms, mandated controls, inspection and adjustment, data breach reporting (see later on Security)

APP8: What might be “disclosure”?

Draft guidelines say:

“...an APP entity will generally disclose personal information when it **releases the subsequent handling of the personal information from its effective control**”

- Examples of where APP8 **will** apply from Guidelines:
 - retailer offshores fulfilment to overseas contractor
 - reference checks done by overseas service provider
 - technical and billing support provided from offshore
- But what conditions apply to these arrangements?

What might be “use”?

Draft guidelines say use generally happens when “an APP entity “handles and manages that information within the entity”

- However examples point to “limited circumstances”, “limited purpose” and strict conditions
- Restrictions indicating “use”:
 - limit service provider to “storage and managing”
 - retain right to access, change and retrieve information
 - impose security measures
 - require subcontractors to be subject to same conditions.

Compare “collection” and “holds”

- “collection” includes “...for inclusion in a record” and “record” includes “a document” and “an electronic or other device”.
- Can an offshore provider be a user (not subject to 8.1) but have made a collection? – **No outside the jurisdiction**
- Can an onshore provider be a user (not a person to whom a disclosure is usually made) but have made a collection? – **Yes but is it practicable to comply with APP5?**
- App 11 imposes security obligations on an APP Entity that “holds” Personal Information.

Issues for APP8

- When is third party access “use” not “disclosure”?
- Consider the difference between complying with APP8.1 and imposing conditions that = use:
 - how is your contract different in practice?
 - is there a reason to prefer “use” over “disclosure”?



Implications of “use” vs. “disclosure”

- Cross-border access that is “use”:
 - is not subject 16C!
 - need not be mentioned in a collection notice
 - the fact of “disclosure” and likely place of disclosure need not be mentioned in your Privacy Policy
- What are the implications if this distinction for onshore sub-contractors?



APP 11: Security of personal information

APP 11.1:

If an App Entity **holds** personal information , the entity must take such steps as are reasonable in the circumstances to protect the information:

- a) from misuse, interference and loss; and
- b) from unauthorized access modification or disclosure



See also 20Q in relation to credit reporting information.

OAIC draft guidelines

- “active measures”
- “holds” means possession or control

Considerations:

sensitivity of data, level of damage if released, practicability of measure, whether measure is privacy invasive

Possible steps:

governance, ICT security, data breaches, physical security, personal security and training, workplace policies, information life cycle, standards, regular monitoring and review

OAIC Guide to Information Security (4/13)

ICT security:

whitelisting and blacklisting, software security, access, encryption, network security, testing, backing up, communications security

– Examples:

- Vodafone (p10)
- Medicare (p11)
- Telstra (p13)
- Medical Centre (14)

APP11.2: Personal Information no longer needed

- If an APP entity holds personal information;
 - the information is no longer needed for any purpose for which it may be used or disclosed; and
 - not a Commonwealth record or required by law or tribunal; then
 - the APP entity must take reasonable steps to destroy or de-identify the information.
- Consider the practical challenge of making this assessment on all information held



Credit Provider rules

Introduction

Credit reporting under the **new** privacy regime

- ✓ New types of personal information permitted in the credit reporting system
- ✓ Includes non-default credit data about a customer (i.e., credit exposure, not just defaults)
- ✓ Enhanced privacy protection (access, correction, complaints)
- ✓ Credit providers must be members of an EDR scheme
- ✓ A comprehensive Credit Reporting Code

Which entities are bound

- Credit reporting bodies (CRB)
- Credit providers (CP)
- Affected information recipients (AIR)

The distinctions between these bodies is important because the classification of the body will determine how, and to what extent, the credit reporting provisions apply to the body.

What are Credit Providers?

- Banks, non-bank lenders, non-bank credit card providers
- Organisations that:
 - Provide credit in relation to the provision of goods or services and extend the terms of the credit **beyond 7 days**; or
 - Hire, lease or rent goods for **7 days** without a deposit of at least the value of the goods
 - Are CPs in relation to that credit aspect only

What are Credit Providers?

- Organisations involved in a securitisation arrangement
- Organisations who acquire the rights of a CP in relation to the repayment of an amount of credit
- Agents of CPs



Credit info is...

- Identification information
- Consumer credit liability information
- Repayment history information
- Statement that an information request has been made in relation to the individual by a CP
- Type of credit and amount of credit sought in an application
- Default information
- Payment information
- New arrangement information
- Court proceedings information
- Personal insolvency information
- Publicly available information that relates to the individuals' activities in Australia and their credit worthiness
- Opinion of the CP that the individual has committed a serious credit infringement

The 5 new data sets

1 Type of consumer credit

2 Day on which consumer credit is entered into and day on which it is terminated

3 Terms and conditions of the consumer credit that relate to repayment)

4 Credit limit

5 Repayment history information (including payment history)

New categories of info

- Credit information
- Credit reporting information
- CP derived information
- Credit reporting information that is de-identified
- A pre-screening assessment

A distinction is drawn between these different classes of information because the credit reporting regime imposes different privacy requirements for each category (although they may sometimes overlap)

Interaction between Part IIIA, APPs & CR Code

CRB = APPs do not apply. Only Part IIIA applies.

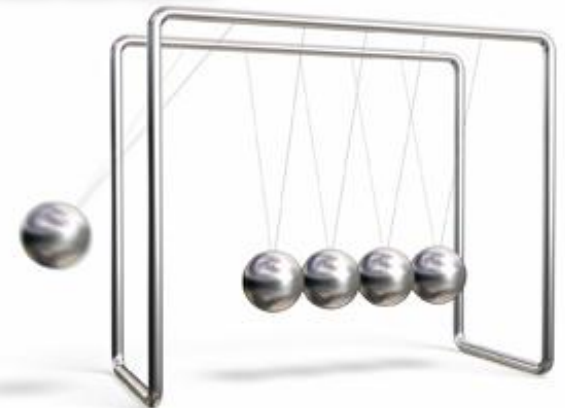
CP = APPs apply alongside Part IIIA + CR Code

AIR = APPs apply alongside Part IIIA + CR Code









Additional layer of compliance

Credit Reporting Code adds to aspects of the credit reporting obligations imposed by Part IIIA of the Privacy Act and the Privacy Regulation 2013.

Compliance with the CR Code alone will not achieve full compliance with Part IIIA.



What's new with CR Compliance?

-  **Must have** Credit Reporting Policy
-  **Must notify** customers about disclosures to CRB
-  **Must give** regulated notices to customers in relation to credit reporting/disclosure to CRBs e.g. default info, payment info
-  **Must only** use and disclose credit related info **within** the Credit Reporting System participants
-  **Can** disclose to bodies that do not have an Australian link **but ultimately** liable for any breaches;
-  **Must have** systems to maintain quality & security of info
-  **Must have** procedures to deal with access and correction requests
-  **Must have** a complaints handling process

CHECKLIST

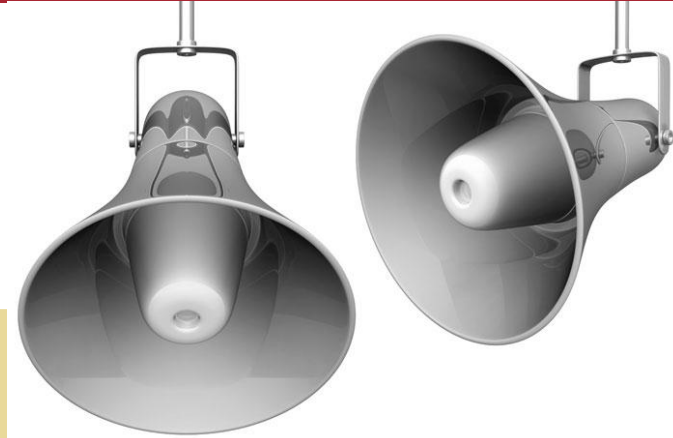


Details on what's new for CPs...

- Must have comprehensive credit reporting compliance plan (can be audited at any time by a CRB)
- Must be a member of an EDR scheme
- Must provide the regulated notices under Part IIIA. Examples:
 - Notice declining an application for credit
 - “Section 6Q” & “section 21D(3)(d)” notice of disclosure of default info
 - Notice of disclosure of consumer credit liability info to CRB
- Must “coordinate” interaction between Part IIIA and the National Consumer Credit Protection Act
 - Dealing with hardship applications, default notices etc

To do list

What do your contracts say?

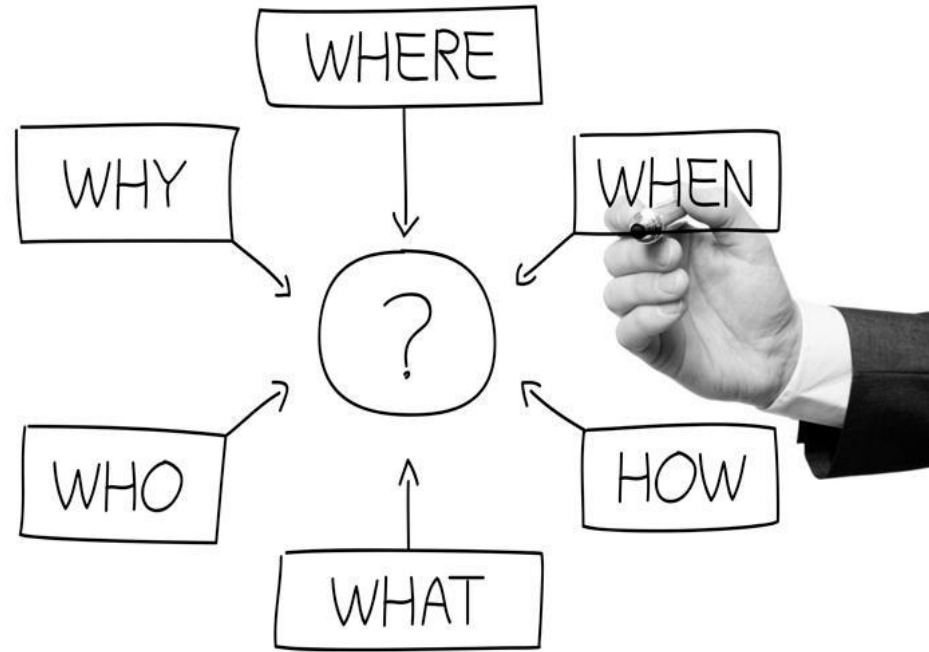


- Consider contracts with customers and contracts with suppliers
- No sub-contracting without approval?
- No offshoring (listed exceptions?)
- Security obligations related to transmissions and malicious code?
- Security regarding personnel, white room access, location from which access can take place?, management of workflow/ splitting of tasks?
- What is support able to see? What can external providers see and change?
- Do you control access permissions and have tracking?

To do list

Steps required:

- Review and consider current practices
- Design new practices and lines of responsibility that conform with the APPs
- Implement improved procedures and systems for compliance
- Introduce supplementary terms of contract where necessary
- Update privacy policies, collection notices, points of sale, websites, apps etc.
- Undertake training regarding the updated framework
- Reflect changes in new contracts with data processors (on- and off-shore)
- Monitor in operation and adjust to feedback and new circumstances.



Questions and discussion

Conclusion

Contact:

Patrick Fair

patrick.fair@bakermckenzie.com

(02) 89225534

Further info: www.oaic.gov.au