Chapter B:
Key concepts

Version 1.3, July 2019

OAIC

Contents

APP entity 4
Australian Link 6
Carries on business in Australia 6
Carry on business 6
In Australia 7
Personal information collected ‘in Australia’ 8
Collects 8
Commonwealth record 9
Consent 9
Express or implied consent 10
Voluntary 11
Informed 11
Current and specific 11
Capacity 12
De-identification 13
Disclosure 13
Enforcement body 15
Enforcement related activities 16
Health information 16
Health Service 18
Holds 18
Immigration Department 19
Personal information 19
Meaning of 'reasonably identifiable’ 20
Deceased persons 21
Purpose 21
Primary purpose and secondary purpose 21
Reasonable, Reasonably 22
Reasonable steps 23
Reasonably believes 23
Reasonably necessary and necessary 24
Recognised external dispute resolution scheme 24
Registered APP code 25
Related body corporate 25

Required or authorised by or under an Australian law or a court/tribunal order **26**
Meaning of 'required' 26
Meaning of 'authorised' 26
Meaning of 'Australian law' 26
Meaning of 'court/tribunal order' 27
Sensitive information **27**
Use **28**

B.1 This Chapter outlines some key words and phrases that are used in the Privacy Act and the Australian Privacy Principles (APPs).

APP entity

B.2 An 'APP entity' is defined to be an agency or organisation (s 6(1)).

B.3 An 'organisation' is defined to be:

- an individual (including a sole trader)
- a body corporate
- a partnership
- any other unincorporated association, or
- a trust

unless it is a small business operator, registered political party, State or Territory authority or a prescribed instrumentality of a State (s 6C).

B.4 The following terms are also defined in the Privacy Act: 'small business operator' (s 6D), 'registered political party' (s 6(1)) and 'State or Territory authority' (s 6C).

B.5 In general, a small business operator is an individual (including a sole trader), body corporate, partnership, unincorporated association or trust that has an annual turnover of $3,000,000 or less for a financial year, unless an exception applies (s 6D). If an exception applies this kind of business may be an organisation. The exceptions include businesses that:

- provide a health service and hold health information other than in an employee record
- disclose personal information about another individual for a benefit, service or advantage, or provide a benefit, service or advantage to collect personal information about another individual from anyone else, unless they do so with the consent of the individual or are required or authorised by or under legislation to do so
- are contracted service providers for a Commonwealth contract (s 6D(4))

B.6 Following are two examples of how the second exception may apply:

- An example of an entity that discloses personal information for a benefit, service or advantage is an entity that sells a list of personal information to another entity so that the other entity can use that information for the purpose of direct marketing.
- An example of an entity that provides a benefit, service or advantage to collect personal information is a lobby group that pays another entity to collect information about the political preferences of an individual.

B.7 A non-APP entity may be treated as an organisation (and therefore as an APP entity) in certain circumstances, for example, a small business operator that is related to an organisation covered by the Privacy Act (s 6D(9)) or an entity that chooses to be treated as an organisation (s 6EA). Also, some small business operators are treated as organisations (and therefore an APP entity) in relation to the following activities they carry out:

- activities of reporting entities or authorised agents relating to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and its Regulations and Rules (s 6E(1A))

- certain acts and practices in connection with the operation of a residential tenancy database (s 6E(2)) and regulation 7 of Privacy Regulation 2013
- activities related to the conduct of a protection action ballot (s 6E(1)(B))[1]

B.8 'Agency' refers to Australian Government (and Norfolk Island Government) agencies,[2] but does not include State and Territory agencies. An 'agency' is defined to be:

- a Minister
- a Department
- a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment, not being:
  - an incorporated company, society or association; or
  - an organisation that is registered under the Fair Work (Registered Organisations) Act 2009 or a branch of such an organisation
- a body established or appointed by the Governor-General, or by a Minister, other than by or under a Commonwealth enactment
- a person holding or performing the duties of an office established by or under, or an appointment made under, a Commonwealth enactment, other than a person who, by virtue of holding that office, is the Secretary of a Department
- a person holding or performing the duties of an appointment, being an appointment made by the Governor-General, or by a Minister, other than under a Commonwealth enactment
- a federal court
- the Australian Federal Police
- a Norfolk Island agency
- the nominated AGHS company[3]
- an eligible hearing service provider, or
- the service operator under the Healthcare Identifiers Act 2010 (s 6(1))

B.9 Section 6(5) clarifies that a person shall not be taken to be an agency merely because the person is the holder of, or performs the duties of, certain offices, such as a judicial office or of an office of magistrate.

[1] See also, s 6F which describes when a state instrumentality will be treated as an organisation.

[2] The APPs do not apply to Australian Capital Territory Government agencies. The Information Privacy Act 2014 (ACT) regulates how personal information is handled by ACT public sector agencies. This Act includes a set of Territory Privacy Principles, which cover the collection, use, storage and disclosure of personal information, and an individual's access to and correction of that information. For more information about the TPPs, including how they differ from the APPs, see Privacy in the ACT, OAIC website https://www.oaic.gov.au.

[3] Nominated AGHS company means 'a company that (a) is the nominated company (within the meaning of Part 2 of the Hearing Services and AGHS Reform Act 1997); and (b) is either (i) Commonwealth owned (within the meaning of that Part); or (ii) a corporation' (s 6(1)).

Australian Link

B.10 The APPs extend to an act done, or practice engaged in, outside Australia and the external Territories by an organisation, or small business operator, that has an Australian link (s 5B(1A)).

B.11 An organisation or small business operator has an Australian link where it is:

- an Australian citizen or a person whose continued presence in Australia is not subject to a legal time limitation
- a partnership formed, or a trust created, in Australia or an external Territory
- a body corporate incorporated in Australia or an external Territory, or
- an unincorporated association that has its central management and control in Australia or an external Territory (s 5B(2))

B.12 An organisation that does not fall within one of those categories will also have an Australian link where:

- it carries on business in Australia or an external Territory, and
- it collected or held personal information in Australia or an external Territory, either before or at the time of the act or practice (s 5B(3))

Carries on business in Australia

B.13 The phrase 'carries on business in Australia' in s 5B(3)(c) is not defined in the Privacy Act. However, it arises in other areas of law, including corporations and consumer law. Guidance may be drawn from judicial consideration of the phrase in those contexts.

B.14 The two elements — 'carries on business' and 'in Australia' — are connected but can be considered separately. Australian courts have held that both are questions of fact.[4] An assessment should be made having regard to all relevant circumstances, particularly the nature of the enterprise conducted by an entity, and the particular Act being applied.[5] In this instance, it is the Privacy Act being applied.

Carry on business

B.15 The general law concept of 'carrying on business' has been said to 'generally involve conducting some form of commercial enterprise, systematically and regularly with a view to profit'[6]; or to embrace 'activities undertaken as a commercial enterprise in the nature of a going concern, that is, activities engaged in for the purpose of profit on a continuous and repetitive basis'.[7]

B.16 The focus of those definitions upon conducting or establishing a commercial enterprise for the purpose of profit is important. Nevertheless, a necessary modification of the concept in

[4] See Luckins v Highway Motel (Carnavon) Pty Ltd (1975) 133 CLR 164, per Stephen J, at [186]; Bray v F Hoffman-La Roche Ltd (2002) 118 FCR 1; ASIC v Active Super (No 1) [2012] FCA 1519 at [47]

[5] See ASIC v Edwards [2004] QSC 344 at [62]; Eltran Pty Ltd v Starport Futures Trading Corporation [2009] QSC 94 at [8]

[6] Gebo Investments (Labuan) Ltd v Signatory Investments Pty Ltd [2005] NSWSC 544, at [38]

[7] Hope v Council of the City of Bathurst (1980) 144 CLR 1 at [8]. For a discussion of the indicia of a 'business', see On Call Interpreters and Translators Agency Pty Ltd v Commissioner of Taxation (No 3) [2011] FCA 366 at [217] – [281]

the context of the Privacy Act is that the Act can apply to a non-profit entity that is an 'organisation' as defined in s 6C(1). As to those entities, the more important element may be the repetition of commercial acts on a systematic or continuing basis as part of the activities of the entity.

In Australia

B.17 Whether a business is carried on 'in Australia' focusses upon whether activity is undertaken in Australia as part of the entity's business. There is 'a need for some physical activity in Australia through human instrumentalities, being activity that itself forms part of the course of conducting business'.[8] However, as noted in another decision, 'provided that there are acts within Australia which are part of the company's business, the company will be doing business in Australia although the bulk of its business is conducted elsewhere and it maintains no office in Australia'.[9]

B.18 An important consideration in applying this territorial requirement in the context of the Privacy Act is that the Act, though technologically-neutral, operates in an environment where personal information is regularly collected, held, used and disclosed online by organisations that may simultaneously carry on business through the web in many countries. In addition, an object of the Privacy Act is to 'promote the protection of the privacy of individuals' (s 2A(a)), which requires that regard be had to contemporary and practical circumstances.

B.19 In this context, factors that may be considered in assessing if an entity carries on business in Australia include whether:

- the entity has a place of business in Australia
- people who undertake business acts for the entity are located in Australia – for example, an entity may carry on business in Australia where an agent acting on its behalf carries on its business from some fixed place in Australia[10]
- the entity has a website that offers goods or services to countries including Australia
- Australia is one of the countries on the drop-down menu appearing on the entity's website
- web content that forms part of carrying on the business, was uploaded by or on behalf of the entity, in Australia
- business or purchase orders are assessed or acted upon in Australia
- the entity is the registered proprietor of trademarks in Australia[11]

B.20 The presence or absence of one of these factors may not be determinative in assessing whether an entity carries on business in Australia. For example, where an entity does not have a place of business in Australia, this does not necessarily mean that it does not carry on business in Australia.

[8] Gebo Investments (Labuan) Ltd v Signatory Investments Pty Ltd [2005] NSWSC 544 at [33]

[9] Australian Securities and Investments Commission v ActiveSuper Pty Ltd (No 1) [2012] FCA 1519 at [47]

[10] Bray v F Hoffman-La Roche Ltd (2002) 118 FCR 1 at [62]

[11] Australian Wool Innovation Ltd v Newkirk (no 3) [2005] FCA 1308 at [34]

B.21 An entity will not generally be regarded as carrying on business in Australia solely on the basis that a purchase order can be placed in Australia or that it has a website that can be accessed from Australia.[12]

Personal information collected 'in Australia'

B.22 Personal information is collected 'in Australia' under s 5B(3)(c), if it is collected from an individual who is physically present in Australia or an external Territory, regardless of where the collecting entity is located or incorporated. An example is the collection of personal information from an individual who is physically located in Australia or an external Territory, via a website that is hosted outside Australia. This applies even if the website is owned by a company that is located outside of Australia or that is not incorporated in Australia.[13]

Collects

B.23 An APP entity collects personal information 'only if the entity collects the personal information for inclusion in a record or generally available publication' (s 6(1)).

B.24 The term 'record' is defined in s 6(1) and includes a document or an electronic or other device. Some items are excluded from the definition, such as anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition, and Commonwealth records in the open access period.

B.25 The term 'generally available publication' is defined in s 6(1) to mean a 'magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public', regardless of the form in which it is published and whether it is available on payment of a fee.

B.26 An APP entity does not collect personal information where that information is acquired but not included in a record or generally available publication. For example, a newspaper article containing personal information will not be 'collected' by the entity unless, for example, a clipping of the article is kept and stored with other documents held by the entity or the article is scanned and saved into the entity's electronic database.

B.27 The concept of 'collection' applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means, including from:

- individuals
- other entities
- generally available publications
- surveillance cameras, where an individual is identifiable or reasonably identifiable
- information associated with web browsing, such as personal information collected by cookies[14]
- biometric technology, such as voice or facial recognition

[12] Gebo Investments (Labuan) Ltd v Signatory Investments Pty Ltd [2005] NSWSC 544

[13] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 218.

[14] Analytical information collected from cookies (e.g., the number of times a page was visited) will not be personal information under the Privacy Act unless an individual is reasonably identifiable (see paragraphs B.85–B.96 below).

B.28 Collection may also take place when an APP entity generates personal information from other data it holds, such as the generation of an audit log.

Commonwealth record

B.29 A 'Commonwealth record' has the same meaning as in the Archives Act 1983 (Archives Act) (s 6(1)).

B.30 The Archives Act states that a 'Commonwealth record' means:

- a record[15] that is the property of the Commonwealth or a Commonwealth institution, or
- a record that is deemed to be a Commonwealth record either by a regulation made under the Archives Act or under s 22 of the Archives Act (which applies to records kept by a Royal Commission or Commission of inquiry) (s 3(1))

B.31 Some categories of records are excluded from that definition:

- 'exempt material', which includes, for example, material included in the memorial collection of the Australian War Memorial, and material included in the collections maintained by the National Library of Australia, the National Gallery of Australia, the National Portrait Gallery of Australia, and the National Museum of Australia
- a register or guide maintained by the Archives, namely, the Australian National Register of Records, Australian National Guide to Archival Material or Australian National Register of Research Involving Archives (see Part VIII, Archives Act)

B.32 It is likely that all or most personal information collected or received by an agency will be included in a 'Commonwealth record'. Where an organisation is a contracted service provider under a Commonwealth contract, the records collected, received or held by that organisation under the contract may also be Commonwealth records.

B.33 APPs 4.3 and 11.2 require the destruction or de-identification of personal information in certain circumstances (see Chapters 4 and 11). These requirements do not apply to information contained in a Commonwealth record. Retention, destruction and alteration of Commonwealth records is governed by the Archives Act. A Commonwealth record can, as a general rule, only be destroyed or altered in accordance with s 24 of the Archives Act. The grounds on which this may be done include with the permission of the National Archives of Australia (as set out in a records disposal authority) or in accordance with 'normal administrative practice'. Further information about Archives Act requirements is available from the National Archives of Australia at <www.naa.gov.au>.

Consent

B.34 Consent is relevant to the operation of a number of APPs. In some, consent is an exception to a general prohibition against personal information being handled in a particular way (for

[15] 'Record' is defined in s 3(1) of the Archives Act as 'a document, or an object, in any form (including any electronic form) that is, or has been, kept by reason of: (a) any information or matter that it contains or that can be obtained from it; or (b) its connection with any event, person, circumstance or thing'.

example, APPs 3.3(a) and 6.1(a)). In others, consent provides authority to handle personal information in a particular way (for example, APPs 7.3, 7.4 and 8.2(b)).

B.35 Consent means 'express consent or implied consent' (s 6(1)). The four key elements of consent are:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent

Express or implied consent

B.36 Express consent is given explicitly, either orally or in writing. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.

B.37 Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.

B.38 An APP entity should not assume that an individual has consented to a collection, use or disclosure that appears to be advantageous to that person. Nor can an entity establish implied consent by asserting that if the individual knew about the benefits of the collection, use or disclosure, they would probably consent to it.

B.39 Generally, it should not be assumed that an individual has given consent on the basis alone that they did not object to a proposal to handle personal information in a particular way. An APP entity cannot infer consent simply because it provided an individual with notice of a proposed collection, use or disclosure of personal information. It will be difficult for an entity to establish that an individual's silence can be taken as consent. Consent may not be implied if an individual's intent is ambiguous or there is reasonable doubt about the individual's intention.

B.40 Use of an opt-out mechanism to infer an individual's consent will only be appropriate in limited circumstances, as the individual's intention in failing to opt-out may be ambiguous. An APP entity will be in a better position to establish the individual's implied consent the more that the following factors, where relevant, are met:

- the opt out option was clearly and prominently presented
- it is likely that the individual received and read the information about the proposed collection, use or disclosure, and the option to opt out
- the individual was given information on the implications of not opting out
- the opt out option was freely available and not bundled with other purposes
- it was easy for the individual to exercise the option to opt out, for example, there was little or no financial cost or effort required by the individual
- the consequences of failing to opt out are not serious
- an individual who opts out at a later time will, as far as practicable, be placed in the position as if they had opted out earlier

B.41 An APP entity should generally seek express consent from an individual before handling the individual's sensitive information, given the greater privacy impact this could have.

B.42 An APP entity should as far as practicable implement procedures and systems to obtain and record consent. This may resolve any doubt about whether consent was given (either on the basis of express or implied consent).

Voluntary

B.43 Consent is voluntary if an individual has a genuine opportunity to provide or withhold consent. Consent is not voluntary where there is duress, coercion or pressure that could overpower the person's will.

B.44 Factors relevant to deciding whether consent is voluntary include:

- the alternatives open to the individual, if they choose not to consent
- the seriousness of any consequences if an individual refuses to consent
- any adverse consequences for family members or associates of the individual if the individual refuses to consent

Bundled consent

B.45 Bundled consent refers to the practice of an APP entity 'bundling' together multiple requests for an individual's consent to a wide range of collections, uses and disclosures of personal information, without giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not.

B.46 This practice has the potential to undermine the voluntary nature of the consent. If a bundled consent is contemplated, an APP entity could consider whether:

- it is practicable and reasonable to give the individual the opportunity to refuse consent to one or more proposed collections, uses and/or disclosures
- the individual will be sufficiently informed about each of the proposed collections, uses and/or disclosures
- the individual will be advised of the consequences (if any) of failing to consent to one or more of the proposed collections, uses and/or disclosures (see also, discussion of 'informed' below)

Informed

B.47 An individual must be aware of the implications of providing or withholding consent, for example, whether access to a service will be denied if consent is not given to collection of a specific item of personal information. An APP entity should ensure that an individual is properly and clearly informed about how their personal information will be handled, so they can decide whether to give consent (see also, discussion of 'capacity' below). The information should be written in plain English, without legal or industry jargon.

Current and specific

B.48 An APP entity should generally seek consent from an individual for collection and proposed uses and disclosures of personal information at the time the information is collected. Alternatively, if consent was not sought at the time of collection, or that consent did not cover a proposed use or disclosure, an entity should seek the individual's consent at the time of the use or disclosure.

B.49 Consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely. It is good practice to inform the individual of the period for which the consent will be relied on in the absence of a material change of circumstances.

B.50 An APP entity should not seek a broader consent than is necessary for its purposes, for example, consent for undefined future uses, or consent to 'all legitimate uses or disclosures' (see also, discussion of 'bundled consent' above). When seeking consent, an entity should describe the purpose to which it relates. The level of specificity required will depend on the circumstances, including the sensitivity of the personal information.

B.51 An individual may withdraw their consent at any time, and this should be an easy and accessible process. Once an individual has withdrawn consent, an APP entity can no longer rely on that past consent for any future use or disclosure of the individual's personal information. Individuals should be made aware of the potential implications of withdrawing consent, such as no longer being able to access a service.

Capacity

B.52 An individual must have the capacity to consent. This means that the individual is capable of understanding the nature of a consent decision, including the effect of giving or withholding consent, forming a view based on reasoned judgement and how to communicate a consent decision. An APP entity can ordinarily presume that an individual has the capacity to consent, unless there is something to alert it otherwise, for example, the individual is a child or young person (see below). If an entity is uncertain as to whether an individual has capacity to consent at a particular time, it should not rely on any statement of consent given by the individual at that time.

B.53 Issues that could affect an individual's capacity to consent include:

- age
- physical or mental disability
- temporary incapacity, for example during a psychotic episode, a temporary psychiatric illness, or because the individual is unconscious, in severe distress or suffering dementia
- limited understanding of English

B.54 An APP entity should consider whether any such issue could be addressed by providing the individual with appropriate support to enable them to have capacity to consent. If an individual does not have capacity to consent, even with support or the provision of additional resources such as an interpreter or alternative communication methods, and consent is required, an entity should consider who can act on the individual's behalf. Options include:

- a guardian
- someone with an enduring power of attorney
- a person recognised by other relevant laws, for example in NSW, a 'person responsible' under the Guardianship Act 1987 (NSW) (this may be an individual's spouse, partner, carer, family member or close friend), or
- a person who has been nominated in writing by the individual while they were capable of giving consent

B.55 An individual who lacks the capacity to consent should nevertheless be involved, as far as practicable, in any decision-making process. To the extent practicable in the circumstances,

an APP entity should ensure that privacy issues are discussed with individuals who have impaired decision-making capacity in a way that is understandable and comprehensible.

Children and young people

B.56 The Privacy Act does not specify an age after which individuals can make their own privacy decisions. An APP entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent.

B.57 As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.

B.58 If it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.

De-identification

B.59 Personal information is de-identified 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable' (s 6(1)). De-identified information is not 'personal information' (see paragraphs B.85–B.96).

B.60 De-identification involves removing or altering information that identifies an individual or is reasonably likely to do so. Generally, de-identification includes two steps:

- removing personal identifiers, such as an individual's name, address, date of birth or other identifying information, and
- removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification

B.61 De-identification may not altogether remove the risk that an individual can be re-identified. There may, for example, be a possibility that another dataset or other information could be matched with the de-identified information. The risk of re-identification must be actively assessed and managed to mitigate this risk. Relevant factors to consider when determining whether information has been effectively de-identified could include the cost, difficulty, practicality and likelihood of re-identification.[16]

B.62 For more information on when and how to de-identify information, and how to manage and mitigate the risk of re-identification, see De-identification and the Privacy Act.[17]

Disclosure

B.63 Disclosure is not defined in the Privacy Act.

[16] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 60.

[17] OAIC, De-identification and the Privacy Act, OAIC website <https://www.oaic.gov.au>.

B.64 An APP entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control. This focuses on the act done by the disclosing party, and not on the actions or knowledge of the recipient. Disclosure, in the context of the Privacy Act, can occur even where the personal information is already known to the recipient.[18]

B.65 The release may be a proactive release, a release in response to a specific request, an accidental release or an unauthorised release by an employee.

B.66 Examples include where an APP entity:

- 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[19] and it is accessible to another entity or individual
- accidentally provides personal information to an unintended recipient[20]
- displays a computer screen so that the personal information can be read by another entity or individual, for example at a reception counter or in an office

B.67 Where an APP entity engages a contractor to perform services on its behalf, the provision of personal information to that contractor will in most circumstances be a disclosure (see paragraph B.144 for the limited circumstances where it will be a 'use').

B.68 'Disclosure' is a separate concept from:

- 'unauthorised access' which is addressed in APP 11. An APP entity is not taken to have disclosed personal information where a third party intentionally exploits the entity's security measures and gains unauthorised access to the information.[21] Examples include unauthorised access following a cyber-attack[22] or a theft, including where the third party then makes that personal information available to others outside the entity. However, where a third party gains unauthorised access, the entity may breach APP 11 if it did not take reasonable steps to protect the personal information from unauthorised access (see Chapter 11 (APP 11)).
- 'use', which is discussed in paragraphs B.142–B.144 below. The concept of 'use' encompasses information handling and management activities occurring within an entity's effective control, for example, when staff of an entity access, read, exchange or make decisions based on personal information the entity holds.

B.69 In a number of APPs the same requirements apply to the 'use' or 'disclosure' of personal information (for example, APP 6.1 (see Chapter 6), APP 7 (see Chapter 7), APP 9.2 (see Chapter 9) and APP 10.2 (see Chapter 10)). For these, it is not necessary to distinguish

---

[18] For a similar approach to interpreting 'disclosure', see Pratt Consolidated Holdings Pty Ltd v Commissioner of Taxation [2011] AATA 907 at [112] – 119]

[19] See OAIC, Medvet Science Pty Ltd: Own motion investigation report, July 2012, OAIC website <https://www.oaic.gov.au>; Telstra Corporation Limited: Own motion investigation report, June 2012, OAIC website <https://www.oaic.gov.au>.

[20] The APP entity may also breach APP 11 if it did not take reasonable steps to protect the information from this unauthorised disclosure (see APP 11, Chapter 11).

[21] The actions of an employee will be attributed to the APP entity where it was carried out 'in the performance of the duties of the person's employment' (s 8(1)).

[22] See OAIC, Sony PlayStation Network / Qriocity: Own motion investigation report, September 2011, OAIC website <https://www.oaic.gov.au>.

between a 'use' and a 'disclosure'. However, the distinction is relevant to the following principles and exceptions that only apply to the 'disclosure' of personal information, and not to its 'use':

- section 16B(5) (see Chapter D)
- APP 1.4(f) and (g) (see Chapter 1)
- APP 5.2(f), (i) and (j) (see Chapter 5)
- APP 6.3 (see Chapter 6)
- APP 8 (see Chapter 8)
- APP 11.1(b) (Chapter 11)

Enforcement body

B.70 'Enforcement body' is defined to mean:

- the Australian Federal Police
- the Integrity Commissioner
- the Australian Crime Commission
- the CrimTrac Agency
- Customs
- the Immigration Department
- the Australian Prudential Regulation Authority
- the Australian Securities and Investments Commission
- the Office of the Director of Public Prosecutions, or a similar body established under a law of a State or Territory
- another Commonwealth agency, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law
- another Commonwealth agency, to the extent that it is responsible for administering a law relating to the protection of the public revenue
- a police force or service of a State or a Territory
- the New South Wales Crime Commission
- the Independent Commission Against Corruption of New South Wales
- the Police Integrity Commission of New South Wales
- the Office of Police Integrity of Victoria
- the Crime and Misconduct Commission of Queensland
- the Corruption and Crime Commission of Western Australia
- another prescribed authority or body that is established under a law of a State or Territory to conduct criminal investigations or inquiries

- a State or Territory authority, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law, or
- a State or Territory authority, to the extent that it is responsible for administering a law relating to the protection of the public revenue (s 6(1)

Enforcement related activities

B.71 'Enforcement related activity' is defined to mean:

- the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law imposing a penalty or sanction
- the conduct of surveillance activities, intelligence gathering activities or monitoring activities
- the conduct of protective or custodial activities
- the enforcement of laws relating to the confiscation of the proceeds of crime
- the protection of the public revenue
- the prevention, detection, investigation or remedying of misconduct of a serious nature, or other conduct prescribed by the regulations
- the preparation for, or conduct of, proceedings before any court or tribunal, or the implementation of court/tribunal orders (s 6(1))

B.72 This definition recognises that 'enforcement related activities' can include lawful surveillance, intelligence gathering or monitoring activities where there may not be an existing investigation.[23] Those activities are distinct but may also overlap.

B.73 Examples of surveillance activities include optical surveillance of an individual or property where information obtained from that surveillance may lead to an investigation of a criminal offence. Examples of intelligence gathering include the collection of personal information about an individual to detect whether an offence has occurred, or to determine whether to initiate an investigation into that offence; the collection of information about whether an individual is planning to commit an offence and whether there are fellow criminal associates. Examples of monitoring activities include the monitoring by an enforcement body of a person who has presented themself to that body in compliance with a court order.[24]

Health information

B.74 'Health information' is defined to mean:

- information or an opinion, that is also personal information, about:
  - the health or a disability (at any time) of an individual, or

[23] Addendum to the Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 3.

[24] Addendum to the Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 3.

  - an individual's expressed wishes about the future provision of health services to him or her, or
  - a health service provided, or to be provided, to an individual, or
- other personal information collected to provide, or in providing, a health service, or
- other personal information about an individual collected in connection with the donation, or intended donation, by the individual of their body parts, organs or body substances, or
- genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual (s 6(1)). (Other types of genetic information that are not health information fall within the definition of 'sensitive information', discussed at paragraphs B.138–B.141.)

B.75 Examples of health information include:

- information about an individual's physical or mental health
- notes of an individual's symptoms or diagnosis and the treatment given
- specialist reports and test results
- appointment and billing details
- prescriptions and other pharmaceutical purchases
- dental records
- records held by a fitness club about an individual
- information about an individual's suitability for a job, if it reveals information about the individual's health
- an individual's healthcare identifier when it is collected to provide a health service
- any other personal information (such as information about an individual's date of birth, gender, race, sexuality, religion), collected for the purpose of providing a health service

B.76 The definition of 'sensitive information' in s 6(1) includes health information. Sensitive information, including health information, attracts additional privacy protections compared to other types of personal information (see for example, APP 3 in Chapter 3). There are also a number of provisions and APPs that deal specifically with health information, including the 'permitted health situation' exceptions set out in s 16B (see Chapter D (Permitted health situations)).

Health Service

B.77 'Health service' is defined to mean:

- an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:
  - to assess, record, maintain or improve the individual's health, or
  - to diagnose the individual's illness or disability, or
  - to treat the individual's illness or disability or suspected illness or disability, or
- the dispensing or prescription of a drug or medicinal preparation by a pharmacist (s 6(1))

B.78 The Privacy Act generally applies to all organisations that provide a health service, including an organisation that is a small business.[25] Examples of organisations that provide a health service include:

- traditional health service providers, such as private hospitals, day surgeries, medical practitioners, pharmacists and allied health professionals
- complementary therapists, such as naturopaths and chiropractors
- gyms and weight loss clinics
- child care centres, private schools and private tertiary educational institutions

Holds

B.79 An APP entity 'holds' personal information if 'the entity has possession or control of a record that contains the personal information' (s 6(1)).

B.80 The term 'record' is defined in s 6(1) and includes a document or an electronic or other device. Some items are excluded from the definition, such as anything kept in a library, art gallery or museum for the purposes of reference study or exhibition and Commonwealth records in the open access period.

B.81 The term 'holds' extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with. Whether an APP entity 'holds' a particular item of personal information may therefore depend on the particular information collection, management and storage arrangements it has adopted. For example, an APP entity 'holds' personal information where:

- it physically possesses a record containing the personal information and can access that information physically or by use of an electronic device (such as decryption software)
- it has the right or power to deal with the personal information, even if it does not physically possess or own the medium on which the personal information is stored. For

[25] Small businesses – namely, those with an annual turnover of $3 million or less – are generally exempt from the operation of the Privacy Act (s 6D). However, this exemption does not apply to an individual, body corporate, partnership, unincorporated association or trust that provides a health service to another individual and holds any health information except in an employee record (s 6D(4)(b)).

example, the entity has outsourced the storage of personal information to a third party but it retains the right to deal with it, including to access and amend that information

B.82 An agency that has placed a record of personal information in the care of the National Archives of Australia, or in the custody of the Australian War Memorial, is considered to be the agency that holds the record for the purposes of the Privacy Act (s 10(4)).

Immigration Department

B.83 'Immigration Department' means 'the Department administered by the Minister administering the Migration Act 1958' (s 6(1)). Information about the particular Minister and Department that administer the Migration Act 1958 can be found on the Federal Register of Legislation.[26]

B.84 The definition of 'enforcement body' includes the 'Immigration Department' (see paragraph B.70). This means that the exception in APP 3.4(d)(i) that permits the collection of sensitive information, and the exceptions in APPS 6.2(e) and 8.2(f) that permit the use and disclosure of personal information, extend to the 'enforcement related activities' of the Immigration Department (see Chapters 3, 6 and 8).[27]

Personal information

B.85 'Personal information' is defined as any '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 a material form or not' (s 6(1))

B.86 Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details, employment details and commentary or opinion about a person.

B.87 Personal information of one individual may also be personal information of another individual. Examples include a marriage certificate that contains personal information of both parties to a marriage, and a vocational reference that includes personal information about both the author and the subject of the reference.

B.88 The personal information 'about' an individual may be broader than the item of information that identifies them. For example, a vocational reference or assessment may comment on a person's career, performance, attitudes and aptitude. Similarly, the views expressed by the author of the reference may also be personal information about the author.

B.89 Personal information that has been de-identified will no longer be personal information. Personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable (see paragraph B.59).

---

[26] See Federal Register of Legislation website <https://www.legislation.gov.au/Series/C1958A00062>.

[27] For examples of the functions and activities of the Immigration Department that will be covered by the 'enforcement related activity' exceptions in APPs 3.4, 6.2 and 8.2, see Addendum to the Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 2.

B.90 What constitutes personal information will vary, depending on whether an individual can be identified or is reasonably identifiable in the particular circumstances.

Meaning of 'reasonably identifiable'

B.91 Whether an individual is 'reasonably identifiable' from particular information will depend on considerations that include:[28]

- the nature and amount of information
- the circumstances of its receipt
- who will have access to the information
- other information either held by or available to the APP entity that holds the information
- whether it is possible for the individual or entity that holds the information to identify the individual, using available resources (including other information available to that individual or entity). Where it may be possible to identify an individual using available resources, the practicability, including the time and cost involved, will be relevant to deciding whether an individual is 'reasonably identifiable'[29]
- if the information is publically released, whether a reasonable member of the public who accesses that information would be able to identify the individual

B.92 The following are given as examples of how those considerations may apply to particular items of information:

- Most entities and individuals would encounter difficulty in using a licence plate number to identify the registrant of a car, as they would not have access to the car registration database. By contrast, an agency or individual with access to that database may be able to identify the registrant. Accordingly, the licence plate number may be 'personal information' held by that agency or individual, but may not be personal information if held by another entity.
- Information that an unnamed person with a certain medical condition lives in a specific postcode area may not enable the individual to be identified, and would not therefore be personal information. By contrast, it may be personal information if held by an entity or individual with specific knowledge that could link an individual to the medical condition and the postcode.[30]
- A common surname that is shared by many people may not be personal information that would reasonably identify a particular individual. However, combined with other information, such as address or other contact information, it may be personal information

B.93 Whether a person is 'reasonably identifiable' is an objective test that has practical regard to the context in which the issue arises. Even though it may be technically possible to identify an individual from information, if doing so is so impractical that there is almost no likelihood

[28] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 61.

[29] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 61.

[30] Autism Aspergers Advocacy Australia and Department of Families, Housing, Community Services and Indigenous Affairs [2012] AICmr 28 (12 November 2012), see Information Commissioner review decisions, OAIC website <https://www.oaic.gov.au>

of it occurring, the information would not generally be regarded as 'personal information'.[31] An individual may not be reasonably identifiable if the steps required to do so are excessively time-consuming or costly in all the circumstances.

B.94 Where it is unclear whether an individual is 'reasonably identifiable', an APP entity should err on the side of caution and treat the information as personal information.

Deceased persons

B.95 The definition of 'personal information' in s 6(1) refers to information or an opinion about an 'individual.' An 'individual' means 'a natural person' (s 6(1)). The ordinary meaning of 'natural person' does not include deceased persons.[32]

B.96 Information about a deceased person may include information about a living individual and be 'personal information' for the purposes of the Privacy Act. For example, information that a deceased person had an inheritable medical condition may indicate that the deceased person's descendants have an increased risk of that condition. If the descendants are identifiable, that information would be personal information about the descendants. The privacy interests of family members could therefore be considered when handling information about deceased persons.

Purpose

B.97 The purpose of an action is the reason why it is done. The purpose for which an APP entity collects, holds, uses and discloses personal information can be relevant to:

- whether the entity is permitted to collect, use, disclose and retain personal information (APPs 3, 4, 6, 7, and 11)
- the matters that must be included in the entity's APP Privacy Policy (APP 1) and in any collection notice to the individual (APP 5)
- the steps that must be taken to ensure the quality of personal information (APP 10) and to correct incorrect information (APP 13)

Primary purpose and secondary purpose

B.98 The purpose for which an APP entity collects personal information is known as the 'primary purpose' of collection. This is the specific function or activity for which the entity collects the personal information. If an APP entity uses or discloses the personal information for another purpose this is known as a 'secondary purpose'. APP 6 sets out when an APP entity may use or disclose personal information for a secondary purpose (see Chapter 6 (APP 6)).

B.99 Where an APP entity collects personal information directly from an individual, the context will help in identifying the primary purpose of collection. For example, the individual may provide the personal information for a particular purpose, such as buying a particular

[31] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 61.

[32] However, for the purposes of Part VIA, which deals with personal information in emergencies and disasters, the definition of 'individual' in s 6(1)) is taken to include an individual who is not living (s 80G(2)).

product or receiving a particular service. This is the primary purpose of collection, even if the entity has additional secondary purposes in mind.

B.100 Where an APP entity receives unsolicited personal information or collects personal information about an individual from a third party, the context will again be relevant in identifying the primary purpose of collection. It will also be relevant to consider the function or activity which the personal information is reasonably necessary for, or to which it directly relates. In some instances, an APP entity that receives unsolicited personal information and retains it will have no primary purpose of collection. For example, where the entity could not have collected personal information under APP 3.1 but nevertheless retains it under APP 4, because the information is contained in a Commonwealth record, or because it is not lawful or reasonable for the entity to destroy it (see APP 4, Chapter 4).

Describing the primary purpose

B.101 How broadly a purpose can be described will depend on the circumstances and should be determined on a case-by-case basis. In cases of ambiguity, and with a view to protecting individual privacy, the primary purpose for collection, use or disclosure should be construed narrowly rather than expansively.

B.102 The primary purpose may nevertheless be described in general terms, as long as the description is adequate to inform an individual of how the APP entity may use or disclose their personal information. A description – the information will be used 'for the functions of the entity' – would generally be considered too broad. Instead, the primary purpose of collection could be described as to:

- provide a particular banking service
- market particular goods or services , or types of goods or services, to the individual
- assess an applicant's suitability for a job
- assess an applicant's eligibility for a loan
- resolve a complaint
- provide further information about a particular service
- enable an agency to give someone a particular benefit or service

B.103 An APP entity does not need to include in its description internal purposes that form part of normal business practices, such as auditing, business planning, billing or de-identifying personal information.

Reasonable, Reasonably

B.104 The terms 'reasonable' and 'reasonably' are used in the Privacy Act and APPs to qualify a test or obligation. Examples include that 'personal information' is information about an individual who is 'reasonably' identifiable (s 6(1)) and an APP entity must not collect personal information unless it is 'reasonably necessary' for one or more of the entity's functions or activities (APP 3).

B.105 'Reasonable' and 'reasonably' are not defined in the Privacy Act. The terms bear their ordinary meaning, as being based upon or according to reason and capable of sound explanation. What is reasonable is a question of fact in each individual case. It is an objective test that has regard to how a reasonable person, who is properly informed, would be

expected to act in the circumstances. What is reasonable can be influenced by current standards and practices.[33] It is the responsibility of an APP entity to be able to justify that its conduct was reasonable. In a related context, the High Court has observed that whether there are 'reasonable grounds' to support a course of action 'requires the existence of facts which are sufficient to [persuade] a reasonable person';[34] it 'involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question'.[35] As that indicates, there may be a conflicting range of objective circumstances to be considered, and the factors in support of a conclusion should outweigh those against.

B.106 The terms 'reasonable' and 'reasonably' are discussed further in the APP guidelines, as they arise in the context of each of the relevant APPs.

Reasonable steps

B.107 A number of the APPs require an APP entity to 'take such steps as are reasonable in the circumstances' (for example, APP 1.2 (see Chapter 1), APP 8.1 (see Chapter 8) and APP 11(see Chapter 11). The shorthand expression used in the APP guidelines is 'reasonable steps'.[36]

B.108 The 'reasonable steps' test is an objective test, and is to be applied in the same manner as 'reasonable' and 'reasonably'. It is the responsibility of an APP entity to be able to justify that reasonable steps were taken.

B.109 Some APPs require an APP entity to take 'such steps (if any) as are reasonable in the circumstances' (for example, APP 5.1 (see Chapter 5), APP 10 (see Chapter 10), APP 12.5 (see Chapter 12), APPs 13.1 and 13.2 (see Chapter 13). The inclusion of '(if any)' acknowledges that it in some circumstances an entity will satisfy the requirement to take reasonable steps by taking no steps.

Reasonably believes

B.110 A number of the exceptions to the APPs require an APP entity to have a 'reasonable belief' about a particular matter (see for example, APP 3.4 (Chapter 3), APP 6.2(e) (Chapter 6), APP 8.2 (Chapter 8), Permitted general situations, (Chapter C)).

B.111 The phrase 'reasonable belief' is to be applied in the same manner as 'reasonable' and 'reasonably'. That is, the APP entity must have a reasonable basis for the belief, and not merely a genuine or subjective belief. The requirement for a reasonable belief precludes arbitrary action, but may still leave something to surmise or conjecture.[37] It is the responsibility of an entity to be able to justify its reasonable belief.

[33] For example, Jones v Bartlett [2000] HCA 56 [57] – [58] (Gleeson CJ); Bankstown Foundry Pty Ltd v Braistina [1986] HCA 20 [12] (Mason, Wilson and Dawson JJ).

[34] George v Rockett (1990) 170 CLR 104 at 112 (Mason CJ, Brennan, Deane, Dawson, Toohey, Gaudron & McHugh JJ).

[35] McKinnon v Secretary, Department of Treasury (2006) 228 CLR 423 at 430 (Gleeson CJ & Kirby J).

[36] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 54.

[37] George v Rockett (1990) 170 CLR 104 at 112, 116.

Reasonably necessary and necessary

B.112 A number of APPs require a collection, use or disclosure to be 'reasonably necessary' for a particular purpose – see APPs 3, 6, 8 and 9. Certain permitted general situations and permitted health situations refer to a collection, use or disclosure being 'necessary' for a particular purpose (see Chapters C and D), and APP 7 refers to a use or disclosure being 'necessary' to meet a contractual obligation (see Chapter 7).

B.113 The term 'reasonable' is discussed at paragraphs B.104–B.106. 'Necessary' is not defined in the Privacy Act. The High Court of Australia has noted that 'there is, in Australia, a long history of judicial and legislative use of the term 'necessary', not as meaning essential or indispensable, but as meaning reasonably appropriate and adapted'.[38] However, in the context of the Privacy Act, it would not be sufficient if the collection, use or disclosure is merely helpful, desirable or convenient.

B.114 The 'reasonably necessary' test is an objective test: whether a reasonable person who is properly informed would agree that the collection, use or disclosure is necessary. It is the responsibility of an APP entity to be able to justify that the particular collection, use or disclosure is reasonably necessary.

B.115 The test must be applied in a practical sense. For example, under APP 3 if an entity cannot in practice effectively pursue a function or activity without collecting personal information, the collection would usually be considered reasonably necessary for that function or activity. However, a collection, use or disclosure of personal information will not usually be considered reasonably necessary if there are reasonable alternatives available, for example, if de-identified information would be sufficient for the function or activity.

B.116 An APP entity cannot rely solely on normal business practice in assessing whether a collection, use or disclosure is reasonably necessary. The primary issue is whether, in the circumstances of a particular entity, a collection, use or disclosure is reasonably necessary for a particular function or activity.

B.117 The term 'necessary' rather than 'reasonably necessary' is used in certain permitted general situations and permitted health situations, and in APP 7. The context explains this different usage. For example, a permitted health situation may exist if the collection of personal information is 'necessary' for public health research that is conducted in accordance with relevant guidelines. Similarly, APP 7.5 refers to the use or disclosure of personal information for the purpose of direct marketing where that is 'necessary' to meet a contractual obligation. In some of the permitted general situations and permitted health situations the test is whether an APP entity 'reasonably believes' that the collection, use or disclosure of personal information is 'necessary' for a particular purpose, such as lessening or preventing a serious threat to a person's health or safety.

Recognised external dispute resolution scheme

B.118 'Recognised external dispute resolution scheme' is defined as 'an external dispute resolution scheme recognised under section 35A' (s 6(1)).

B.119 Section 35A(1) gives the Information Commissioner power to recognise an external dispute resolution scheme for an entity or a class of entities, or for a specified purpose. A register of

[38] Mulholland v Australian Electoral Commissioner [2004] HCA 41 [39] (Gleeson CJ).

recognised external dispute resolution schemes is maintained on the Office of the Australian Information Commissioner website.[39]

B.120 An individual who considers that an APP entity has interfered with their privacy may complain to a recognised EDR scheme of which the entity is a member, if the complaint falls within the scope of the EDR scheme's recognition. For further discussion of recognised EDR schemes, and their role in handling privacy-related complaints, see Guidelines for Recognising External Dispute Resolution Schemes under s 35A of the Privacy Act.[40]

Registered APP code

B.121 A 'registered APP code' is defined as an APP code that is included on the Codes Register and that is in force (s 26B(1)). A registered APP code is a legislative instrument (s 26B(2)). The requirements in relation to registered APP codes are set out in Division 2 of Part IIIB.

B.122 An 'APP code' is defined as a written code of practice about information privacy (s 26C). It can be developed by an APP entity, either on its own initiative or on request from the Information Commissioner, or by the Information Commissioner directly (ss 26E and 26G). A code may be expressed to apply to all or a specified type of personal information, a specified activity or class of activities of an APP entity, a specified industry sector or professions or specified class of industry sectors or professions, or APP entities that use technology of a specified kind (s 26C(4)).

B.123 The Information Commissioner has power to approve and register an APP code (provided certain conditions are met) by including it on the Codes Register (s 26H).

B.124 Once an APP code is registered, an APP entity bound by the code must not do an act, or engage in a practice, that breaches that code. A breach of a registered APP code will be 'an interference with the privacy of an individual' by the entity under s 13(1)(b).

B.125 A registered APP code does not replace the APPs for the entities which it binds, but operates in addition to the requirements of the APPs.[41] For further discussion about the development of APP codes, and the requirements and process for recognition, see the Guidelines for Developing Codes.[42]

Related body corporate

B.126 Section 6(8) provides that 'the question whether bodies corporate are related to each other is determined in the manner in which that question is determined under the Corporations Act 2001'.

B.127 Section 13B(1) permits related bodies corporate to share personal information (other than sensitive information) in certain circumstances. The effect of s 13B(1) is discussed further in Chapter 3 (APP 3) and Chapter 6 (APP 6).

---

[39] See OAIC website <https://www.oaic.gov.au>.

[40] OAIC, Guidelines for Recognising External Dispute Resolution Schemes, OAIC website <https://www.oaic.gov.au>.

[41] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 199.

[42] OAIC, Guidelines for Developing Codes, OAIC website <https://www.oaic.gov.au>.

Required or authorised by or under an Australian law or a court/tribunal order

B.128 A number of the APPs provide an exception if an APP entity is 'required or authorised by or under an Australian law or a court/tribunal order' to act differently (for example, APP 3.4(a) (Chapter 3), APP 6.2(b) (Chapter 6) and APP 12.3(g) (Chapter 12)). Some other provisions refer more narrowly to an act that is 'required by or under an Australian law (other than this Act)' (s 16B(2) (Chapter D)) or 'required by or under an Australian law, or a court order' (APP 11.2(d) (Chapter 11)), and do not include an act that is 'authorised'.

Meaning of 'required'

B.129 An APP entity that is 'required' by an Australian law or a court/tribunal order to handle information in a particular way has a legal obligation to do so, and cannot choose to act differently. The obligation will usually be indicated by words such as 'must' or 'shall', and may be accompanied by a sanction for non-compliance.

Meaning of 'authorised'

B.130 An APP entity that is 'authorised' under an Australian law or a court/tribunal order has discretion as to whether it will handle information in a particular way. The entity is permitted to take the action but is not required to do so. The authorisation may be indicated by a word such as 'may', but may also be implied rather than expressed in the law or order.

B.131 An APP entity may be impliedly authorised by law to handle personal information in a particular way, where a law requires or authorises a function or activity, and this directly entails the information handling practice. For example, a statute that authorises an APP entity to collect personal information about an individual from a third party implicitly authorises the entity to disclose the individual's identity to the third party.

B.132 An act or practice is not 'authorised' solely because there is no law or court/tribunal order prohibiting it. Nor can an act or practice rely solely on a general or incidental authority conferred by statute upon an agency to do anything necessary or convenient for, or incidental to or consequential upon, the specific functions and powers of the agency. The reason is that the purpose of the APPs is to protect the privacy of individuals by imposing obligations on APP entities in handling personal information. A law will not authorise an exception to those requirements unless it does so by clear and direct language.[43]

Meaning of 'Australian law'

B.133 'Australian law' is defined as:

- an Act of the Commonwealth, or of a State or Territory
- regulations or any other instrument made under such an Act
- a Norfolk Island enactment, or
- a rule of common law or equity (s 6(1))

[43] See Coco v The Queen (1994) 179 CLR 427.

B.134 The definition of Australian law does not include a contract.[44] Consequently, an obligation imposed by contract upon a party to handle information in a particular way will not provide authority for the purposes of the 'required or authorised by or under an Australian law or court/tribunal order' exception.

Meaning of 'court/tribunal order'

B.135 'Court/tribunal order' is defined as an order, direction or other instrument made by a court, a tribunal, a judge, a magistrate, a person acting as a judge or magistrate, a judge or magistrate acting in a personal capacity, and a member or an officer of a tribunal (s 6(1)).

B.136 The definition applies to orders and the like issued by Commonwealth, State and Territory courts, tribunals and members and officers. The definition includes an order, direction or other instrument that is of an interim or interlocutory nature.

B.137 The reference to a judge or a magistrate acting in a personal capacity means that the definition applies to an order or direction issued by a judge or magistrate who has been appointed by government to an office or inquiry that involves the exercise of administrative or executive functions, including functions that are quasi-judicial in nature.[45] An example is a judge who is appointed by government to conduct a royal commission.

Sensitive information

B.138 'Sensitive information' is a subset of personal information and is defined as:

- information or an opinion (that is also personal information) about an individual's:
  - racial or ethnic origin
  - political opinions
  - membership of a political association
  - religious beliefs or affiliations
  - philosophical beliefs
  - membership of a professional or trade association
  - membership of a trade union
  - sexual orientation or practices, or
  - criminal record
- health information about an individual (see paragraphs B.74–B.78)
- genetic information (that is not otherwise health information)
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or
- biometric templates (s 6(1))

B.139 Information may be sensitive information where it clearly implies one of these matters. For example, many surnames have a particular racial or ethnic origin, but that alone will not

[44] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 55.

[45] Drake v Minister for Immigration & Ethnic Affairs (1979) 2 ALD 60; 46 FLR 409; Grollo v Palmer (1995) 184 CLR 348.

constitute sensitive information that clearly indicates the racial or ethnic origin of an individual with that surname.

B.140 Terms such as 'political opinions' and 'philosophical beliefs' are not defined in the Privacy Act. They take their ordinary meaning and should be interpreted broadly. However, not every value, belief or opinion of an individual will be considered to be a political opinion or philosophical belief.

B.141 Sensitive information is generally afforded a higher level of privacy protection under the APPs than other personal information (for example, see APPs 3, 6 and 7). This recognises that inappropriate handling of sensitive information can have adverse consequences for an individual or those associated with the individual. For example, discrimination or mistreatment is sometimes based on a person's race or ethnic origin or union membership. Mishandling of sensitive information may also cause humiliation or embarrassment or undermine an individual's dignity.

Use

B.142 'Use' is not defined in the Privacy Act. Use is a separate concept from disclosure, which is discussed at paragraphs B.63–B.68. As noted at paragraph B.69, many APP requirements apply to both the 'use' and 'disclosure' of personal information, and in those situations it is not necessary to distinguish both concepts.

B.143 Generally, an APP entity uses personal information when it handles and manages that information within the entity's effective control. Examples include:

- the entity accessing and reading the personal information
- the entity searching records for the personal information
- the entity making a decision based on the personal information
- the entity passing the personal information from one part of the entity to another
- unauthorised access by an employee of the entity.[46]

B.144 In limited circumstances, providing personal information to a contractor to perform services on behalf of the APP entity may be a use, rather than a disclosure (see paragraph B.63–B.68). This occurs where the entity does not release the subsequent handling of personal information from its effective control. For example, if an entity provides personal information to a cloud service provider for the limited purpose of performing the services of storing and ensuring the entity may access the personal information, this may be a 'use' by the entity in the following circumstances:

- a binding contract between the entity and the provider requires the provider only to handle the personal information for these limited purposes
- the contract requires any subcontractors to agree to the same obligations, and
- the contract gives the entity effective control of how the information is handled by the provider. Issues to consider include whether the entity retains the right or power to access, change or retrieve the information, who else will be able to access the information and for what purposes, the security measures that will be used for the

[46] An APP entity is taken to have 'used' personal information where an employee gains unauthorised access 'in the performance of the duties of the person's employment' (see s 8(1)).

storage and management of the personal information (see also APP 11.1, Chapter 11) and whether the information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.[47]

[47] For further discussion of cloud computing considerations for agencies, see Secure Cloud Strategy, Digital Transformation Agency website <https://www.dta.gov.au>.