Chapter 3: Australian Privacy Principle 3 — Collection of solicited personal information

Version 1.0, February 2014

Key points

- APP 3 outlines when an APP entity may collect solicited personal information.
- An APP entity solicits personal information if it explicitly requests another entity to provide personal information, or it takes active steps to collect personal information.
- APP 3 deals with when an APP entity can collect personal information, and how an APP entity must collect personal information.
- For personal information (other than sensitive information), an APP entity that is:
    - an agency, may only collect this information where it is reasonably necessary for, or directly related to, the agency's functions or activities
    - an organisation, may only collect this information where it is reasonably necessary for the organisation's functions or activities.
- APP 3 contains different requirements for the collection of sensitive information compared to other types of personal information. Unless an exception applies, an APP entity may only collect sensitive information where the above conditions are met and the individual concerned consents to the collection.
- Personal information must only be collected by lawful and fair means.
- Personal information must be collected from the individual concerned, unless this is unreasonable or impracticable (additional exceptions apply to agencies).

What does APP 3 say?

3.1 The APPs distinguish between an APP entity collecting solicited personal information (APP 3) and receiving unsolicited personal information (APP 4).

3.2 APP 3 deals with two aspects of collecting solicited personal information:

- when an APP entity can collect personal information — the requirements vary according to whether the personal information is or is not sensitive information, and whether the APP entity is an agency or an organisation
- how an APP entity must collect personal information — the same requirements apply to all APP entities and to all kinds of personal information.

3.3 In summary, the principles that apply are:

- an agency may only solicit and collect personal information that is reasonably necessary for, or directly related to, one or more of its functions or activities (APP 3.1)
- an organisation may only solicit and collect personal information that is reasonably necessary for one or more of its functions or activities (APP 3.2)
- in addition to the above requirements, an APP entity may only solicit and collect sensitive information if the individual consents to the sensitive information being collected, unless an exception applies (APP 3.3)

- an APP entity must solicit and collect personal information:
    - only by lawful and fair means (APP 3.5), and
    - directly from the individual, unless an exception applies (APP 3.6).

'Solicit' and 'collect'

3.4 APP 3 applies when an APP entity 'solicits' and 'collects' personal information, while APP 4 applies when an APP entity receives personal information that it 'did not solicit'. Examples of solicited personal information collected by an entity are given in paragraph 3.7 below; examples of unsolicited personal information received by an entity are given in Chapter 4 (APP 4).

3.5 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)). This concept applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means. In practice, all personal information that is held by an entity will generally be treated as information that was collected by the entity. 'Collect' is discussed in more detail in Chapter B (Key concepts).

3.6 An APP entity 'solicits' personal information 'if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included' (s 6(1)). The request may be made to an agency, organisation, individual or a small business operator.[1] A 'request' is an active step taken by an entity to collect personal information, and may not involve direct communication between the entity and an individual.

3.7 Examples of solicited personal information collected by an APP entity include the following, where they are collected for inclusion in a record or generally available publication:

- personal information provided by an individual in response to a request, direction or order
- personal information about an individual provided by another entity in response to a request, direction, order or arrangement for sharing or transferring information between both entities
- personal information provided at a business meeting, where it relates to the subject matter of the meeting, including business cards exchanged at the meeting
- a completed form or application submitted by an individual
- a complaint letter sent in response to a general invitation on an APP entity's website to individuals to complain to the entity
- an employment application sent in response to either a job advertisement published by an entity or an expression of interest register maintained by the entity
- a form completed to enter a competition being conducted by an entity

[1] An 'entity' is defined in s 6(1) to mean an agency, organisation or small business operator. 'Organisation' is defined in s 6C to include an individual.

- personal information provided to a 'fraud hotline' that is designed to capture 'tip-offs' from the public
- an entry in an APP entity's visitors book
- a record of a credit card payment
- CCTV footage that identifies individuals.

Collecting for an APP entity's 'functions or activities'

3.8 An APP entity must only collect personal information which is reasonably necessary for one or more of the entity's functions or activities (APPs 3.1 and 3.2).[2] Agencies may, in addition, collect personal information that is directly related to one or more of the agency's functions or activities.

3.9 Determining whether a particular collection of personal information is permitted involves a two-step process:

- identifying an APP entity's functions or activities - different criteria apply for ascertaining the functions and activities of agencies and organisations
- determining whether the particular collection of personal information is reasonably necessary for (or, for agencies, directly related to) one of those functions or activities.

Identifying the functions or activities of an agency

3.10 An agency's functions will be conferred either by legislation (including a subordinate legislative instrument) or an executive scheme or arrangement established by government. Identifying an agency's functions involves examining the legal instruments that confer or describe the agency's functions. These include:

- Acts and subordinate legislative instruments
- the Administrative Arrangements Order made by the Governor-General
- government decisions or ministerial statements that announce a new government function.[3]

3.11 The activities of an agency will be related to its functions. The activities of an agency include incidental and support activities, such as human resource, corporate administration, property management and public relations activities.

3.12 One resource that describes an agency's functions is that agency's Information Publication Scheme (IPS) entry.[4] Agencies to which the *Freedom of Information Act 1982*

[2] See Chapter 9 (APP 9) for a discussion of particular issues relating to the lawful collection of government related identifiers by organisations.

[3] The source and scope of government functions are discussed at greater length in OAIC, *Guidelines issued by the Australian Information Commissioner under s 93A of the Freedom of Information Act 1982* (at [13.38]–[13.49], OAIC website <www.oaic.gov.au>.

[4] An agency's incidental functions (described in paragraph 3.11) are not required to be published in its IPS entry: see OAIC, *Guidelines issued by the Australian Information Commissioner under s 93A of the Freedom of Information Act 1982* at [13.47]–[13.49], OAIC website <www.oaic.gov.au>.

(FOI Act) applies are required to publish on a website 'details of the functions of the agency'. This forms part of the IPS established by the FOI Act (FOI Act, ss 8(2)(c), 8D(3)). The IPS entries of most agencies are readily accessible through a link on the homepage of the agency's website. Another resource that describes agency functions and activities is the annual report of an agency, usually accessible from the agency's website.

Identifying the functions or activities of an organisation

3.13 An organisation's functions or activities include:

- current functions or activities of the organisation
- proposed functions or activities the organisation has decided to carry out and for which it has established plans
- activities the organisation carries out in support of its other functions and activities, such as human resource, corporate administration, property management and public relations activities.

3.14 The functions and activities of an organisation will commonly be described (though not necessarily exhaustively) on a website, in an annual report, and in corporate brochures, advertising, product disclosure statements and client and customer letters and emails.

3.15 The functions and activities of an organisation (for which it may collect personal information under APP 3) are limited to those in which it may lawfully engage.

Collecting personal information that is 'directly related' to an agency's functions or activities

3.16 An agency may collect personal information that is 'directly related to' one or more of the agency's functions or activities (APP 3.1). To be 'directly related to', a clear and direct connection must exist between the personal information being collected and an agency function or activity.

Collecting personal information that is 'reasonably necessary' for an APP entity's functions or activities

3.17 An APP entity may collect personal information that is 'reasonably necessary for' a function or activity of the entity (APP 3.1 and APP 3.2).[5]

3.18 The 'reasonably necessary' test is an objective test: whether a reasonable person who is properly informed would agree that the collection is necessary. It is the responsibility of an APP entity to be able to justify that the particular collection is reasonably necessary. 'Reasonably necessary' is also discussed in Chapter B (Key concepts).

3.19 Factors relevant to determining whether a collection of personal information is reasonably necessary for a function or activity include:

[5] An APP entity may also collect the personal information of an individual (other than sensitive information) from a related body corporate (s 13B(1)(a)).

- the primary purpose of collection ('purpose' is discussed further in Chapter B (Key concepts)
- how the personal information will be used in undertaking a function or activity of the APP entity (for example, in most circumstances collection on the basis that personal information could become necessary for a function or activity in the future, would not be reasonably necessary)
- whether the entity could undertake the function or activity without collecting that personal information, or by collecting a lesser amount of personal information.

3.20 The following are instances in which the OAIC has previously ruled that a collection of personal information was not reasonably necessary for an entity's function or activity:

- a job applicant being asked to advise if they had suffered a work-related injury or illness, when this was not relevant to the position being advertised[6]
- a person applying to open a bank account being asked to complete a standard form application that included a question about marital status, when this had no bearing on the applicant's eligibility to open an account[7]
- a medical practitioner photographing a patient for the patient's medical file, when this was not necessary to provide a health service.[8]

3.21 Other examples of personal information collection that may not be reasonably necessary for an APP entity's functions or activities include:

- collecting personal information about a group of individuals, when information is only required for some of those individuals
- collecting more personal information than is required for a function or activity. For example, collecting all information entered on an individual's driver licence when the purpose is to establish if the individual is aged 18 years or over
- collecting personal information that is not required for a function or activity but is being entered in a database in case it might be needed in the future (this is to be distinguished from the situation where personal information is required for a function or activity, but is not being used immediately)
- an organisation collecting personal information for or on behalf of a related body corporate where the collection of that personal information is not reasonably necessary for the organisation's own functions or activities.

[6] *Own Motion Investigation v Australian Government Agency* [2007] PrivCmrA 4, Australasian Legal Information Institute website < www.austlii.edu.au >.
[7] *D v Banking Institution* [2006] PrivCmrA 4, Australasian Legal Information Institute website <www.austlii.edu.au>.
[8] *M v Health Service Provider* [2007] PrivCmrA 15, Australasian Legal Information Institute website <www.austlii.edu.au>.

Collecting sensitive information

3.22 APP 3.3 imposes an additional requirement for collecting sensitive information about an individual. Unless an exception applies, an APP entity must:

- satisfy the criteria above, i.e. the collection of the sensitive information must be reasonably necessary for (or, for agencies, directly related to) one or more of the entity's functions or activities, and
- the individual about whom the sensitive information relates must consent to the collection (APP 3.3(a)).

3.23 'Sensitive information' is defined in s 6(1), and is discussed in more detail in Chapter B (Key concepts). 'Consent' is defined in s 6(1) as 'express consent or implied consent', and is discussed in more detail in Chapter B (Key concepts). 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.

3.24 APP 3.4 lists five exceptions to the requirements of APP 3.3(a). These are considered below.

Collecting sensitive information as required or authorised by law

3.25 An APP entity may collect sensitive information if the collection 'is required or authorised by or under an Australian law or a court/tribunal order' (APP 3.4(a)). The meaning of 'required or authorised by or under an Australian law or a court/tribunal order' is discussed in more detail in Chapter B (Key concepts).

3.26 An example of where a law or order may require or authorise collection of sensitive information is the collection by an authorised officer under the *Migration Act 1958* of personal identifiers (that may include biometric information) from a non-citizen who is in immigration detention.[9]

Collecting sensitive information where a permitted general situation exists

3.27 An APP entity may collect sensitive information if a 'permitted general situation' exists in relation to the collection (APP 3.4(b)).

3.28 Section 16A lists seven permitted general situations (two of which apply only to agencies). The seven situations are set out below, and are discussed in Chapter C (Permitted general situations), including the meaning of relevant terms.

Lessening or preventing a serious threat to life, health or safety

3.29 An APP entity may collect sensitive information if:

[9] See *Migration Act 1958*, ss 5A, 261AA.

- it is unreasonable or impracticable to obtain the individual's consent to the collection, and
- the entity reasonably believes the collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (s 16A(1), Item 1).

3.30 Examples of where this permitted general situation might apply are:

- collecting health information about an individual who is seriously injured, requires treatment and, due to their injuries, cannot give informed consent, on the basis that it is impracticable to obtain the individual's consent
- collecting sensitive information about a parent that is required to provide assistance to a child who may be at risk of physical or sexual abuse by the parent, on the basis that it would be unreasonable to obtain the parent's consent.

Taking appropriate action in relation to suspected unlawful activity or serious misconduct

3.31 An APP entity may collect sensitive information if the entity:

- has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being, or may be engaged in, and
- reasonably believes that the collection is necessary in order for the entity to take appropriate action in relation to the matter (s 16A(1), Item 2).

3.32 Examples of where this permitted general situation might apply are the collection of sensitive information by:

- an APP entity that is investigating fraudulent conduct by a professional adviser or a client in relation to the entity's functions or activities
- an agency that is investigating a suspected serious breach by a staff member of the Australian Public Service Code of Conduct.

Locating a person reported as missing

3.33 An APP entity may collect sensitive information if:

- the entity reasonably believes that the collection is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing, and
- the collection complies with rules made by the Information Commissioner under s 16A(2) (s 16A(1), Item 3).

Reasonably necessary for establishing, exercising or defending a legal or equitable claim

3.34 An APP entity may collect sensitive information if the collection is reasonably necessary to establish, exercise or defend a legal or equitable claim (s 16A(1), Item 4).

3.35 An example of where this permitted general situation might apply is an insurer collecting health information about an individual who has made an insurance

compensation claim but is suspected of misrepresenting their claim or the extent of their injuries.[10]

Reasonably necessary for a confidential alternative dispute resolution process

3.36 An APP entity may collect sensitive information if the collection is reasonably necessary for the purposes of a confidential alternative dispute resolution (ADR) process (s 16A(1), Item 5).

3.37 An example of where this permitted general situation might apply is an alternative dispute resolution practitioner making a record of a party recounting their version of events, where that account includes the disclosure of sensitive information about an individual who is directly or indirectly involved in the dispute. This permitted general situation will only apply where the parties to the dispute and the ADR provider are bound by confidentiality obligations.

Necessary for a diplomatic or consular function or activity

3.38 An agency may collect sensitive information if the agency reasonably believes the collection is necessary for the agency's diplomatic or consular functions or activities (s 16A(1), Item 6). This permitted general situation applies only to agencies, and not to organisations.

3.39 An example of where this permitted general situation might apply is where an agency with diplomatic or consular functions collects sensitive information about an individual who is overseas and in need of consular assistance because the individual has been hospitalised, is suffering a psychiatric illness, has been arrested or is missing.

Necessary for certain Defence Force activities outside Australia

3.40 The Defence Force (as defined in s 6(1)) may collect sensitive information if it reasonably believes the collection to be necessary for a warlike operation, peacekeeping, civil aid, humanitarian assistance, a medical emergency, a civil emergency or disaster relief occurring outside Australia and the external Territories (s 16A(1), Item 7).

Collecting sensitive information where a permitted health situation exists

3.41 An organisation may collect sensitive information if a 'permitted health situation' exists in relation to the collection (APP 3.4(c)). This exception applies only to organisations, and not to agencies.

3.42 Section 16B lists two permitted health situations that relate to the collection of health information by an organisation. The two situations are set out below, and are discussed in Chapter D (Permitted health situations), including the meaning of relevant terms.

[10] *N v Law Firm* [2011] AICmrCN 8, OAIC website <www.oaic.gov.au>. See also B v *Law Firm* [2011] PrivCmrA 2 (3 May 2011), viewed 6 March 2013, Australasian Legal Information Institute website <www.austlii.edu.au>.

Providing a health service

3.43 An organisation may collect health information about an individual if the health information is necessary to provide a health service to the individual, and either:

- the collection is required or authorised by or under an Australian law (other than the Privacy Act), or
- the health information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation (s 16B(1)).

3.44 An example of where this permitted health situation might apply is where a participant in the personally controlled electronic health record (e-health record) system collects health information included in a consumer's e-health record as authorised by the *Personally Controlled Electronic Health Records Act 2012*.[11]

3.45 'Health information' is defined in s 6(1) and discussed in more detail in Chapter B (Key concepts).

Conducting research; compiling or analysing statistics; management, funding or monitoring of a health service

3.46 An organisation may collect health information about an individual if the collection is necessary for research relevant to public health or public safety, the compilation or analysis of statistics relevant to public health or public safety, or the management, funding or monitoring of a health service, and:

- the particular purpose cannot be served by collecting de-identified information
- it is impracticable to obtain the individual's consent, and
- the collection is either:
    - required by or under an Australian law (other than the Privacy Act)
    - in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation, or
    - in accordance with guidelines approved under s 95A (s 16B(2)).[12]

3.47 An example of where this permitted health situation might apply is an organisation conducting longitudinal research into heart disease and requiring health information about a large number of individuals from different data sources for research linkage. In this case, the collection must be required by an Australian law or carried out in accordance with the rules or guidelines referred to in s 16B(2).

3.48 'Health information' is defined in s 6(1) and discussed in more detail in Chapter B (Key concepts).

[11] See *Personally Controlled Electronic Health Records Act 2012*, ss 63, 64, 65, 66 and 68.
[12] See National Health and Medical Research Council (NHMRC), *Guidelines approved under Section 95A of the Privacy Act 1988,* NHMRC website <www.nhmrc.gov.au>.

Collecting sensitive information for an enforcement related activity

3.49 An enforcement body may collect sensitive information where:

- if the body is the Immigration Department[13], the Department reasonably believes that collecting the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the Department (APP 3.4(d)(i))
- for other enforcement bodies, the body reasonably believes that collecting the information is reasonably necessary for, or directly related to, one or more of the body's functions or activities (APP 3.4(d)(ii)).

3.50 'Enforcement body' is defined in s 6(1) as a list of specific bodies and is discussed in Chapter B (Key concepts). The list includes Commonwealth, State and Territory bodies that are responsible for policing, criminal investigations, and administering laws to protect the public revenue or to impose penalties or sanctions. Examples of Commonwealth enforcement bodies are the Australian Federal Police, Australian Crime Commission, Customs, the Integrity Commissioner,[14] the Immigration Department, Australian Prudential Regulation Authority, Australian Securities and Investments Commission and AUSTRAC.

3.51 For an enforcement body to collect sensitive information using this exception, it must:

- for the Immigration Department, identify the 'enforcement related activities' it conducts or that are conducted on its behalf, and for other enforcement bodies, identify their 'functions or activities', and
- 'reasonably believe' that the collection is either 'reasonably necessary for' or 'directly related to' one or more of those functions or activities.

3.52 'Reasonably believes' is discussed in more detail in Chapter B (Key concepts). Identifying the 'functions or activities' of an agency is discussed above at paragraphs 3.10–3.12, while 'reasonable necessary for' and 'directly related to' are discussed above at paragraphs 3.16–3.21.

3.53 'Enforcement related activities' are defined in s 6(1) and discussed in Chapter B (Key concepts). Where applied to the Immigration Department, the activities could include assessing and enforcing compliance with visa and citizenship requirements, and detecting, preventing, investigating and prosecuting breaches of visa, immigration and citizenship laws. Non-enforcement related activities of the Department do not fall within this exception.[15]

3.54 An example of where the Immigration Department may collect sensitive information from an individual using this exception is where it reasonably believes that

[13] 'Immigration Department' is defined in s 6(1) as the Department administered by the Minister administering the *Migration Act 1958* and is discussed in Chapter B (Key concepts).
[14] 'Integrity Commissioner' is defined in s 6(1) as having the same meaning as in the *Law Enforcement Integrity Commissioner Act 2006*.
[15] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 76.

the sensitive information directly relates to the function of investigating whether a person has breached an immigration law.

Collection of sensitive information by a non-profit organisation

3.55 A non-profit organisation may collect sensitive information if:

- the information relates to the activities of the organisation, and
- the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities (APP 3.4(e)).

3.56 'Non-profit organisation' is defined in s 6(1) as an organisation 'that is a non-profit organisation; and that engages in activities for cultural, recreational, political, religious, philosophical, professional, trade or trade union purposes'. The term 'cultural purposes' includes both racial and ethnic purposes.

3.57 There are three criteria a non-profit organisation must meet to rely on this exception to collect sensitive information:

- firstly, the non-profit organisation can rely on this exception only when collecting sensitive information for an activity that is undertaken for one of the specified purposes in the definition of 'non-profit organisation' (s 6(1)). An organisation conducting activities for some other purpose cannot rely on this exception to collect sensitive information for that purpose
- secondly, the sensitive information that is collected must 'relate' to the activity that is being conducted for a specified purpose. A clear relationship, assessed objectively, must exist between the information collected and that activity. For example, the information may relate to a fundraising activity undertaken by a non-profit organisation to support its cultural, recreational, political, religious, philosophical, professional, trade or trade union purpose
- thirdly, the sensitive information must relate solely to a member of the organisation, or an individual who has regular contact with the organisation in connection with its activities. Collection of sensitive information about a relative of a member of the organisation would not be covered unless the relative was also a member or person in regular contact with the non-profit organisation.

3.58 An example of where a non-profit organisation may be permitted to collect sensitive information is where a religious organisation collects information about the views of its members on religious or moral issues.

Collecting by lawful and fair means

3.59 An APP entity must collect personal information 'only by lawful and fair means' (APP 3.5). This requirement applies to all APP entities.

Collecting by lawful means

3.60 The term 'lawful' is not defined in the Privacy Act. It is lawful for an organisation to destroy or de-identify unsolicited personal information if it is not unlawful to do so. That is, if the destruction or de-identification is not criminal, illegal or prohibited or proscribed by law. Unlawful activity does not include breach of a contract.

3.61 Examples of collection that would not be lawful include:

- collecting in breach of legislation, for example:
    - collecting via computer hacking[16]
    - collecting using telephone interception or a listening device except under the authority of a warrant[17]
    - requesting or requiring information in connection with, or for the purpose of, an act of discrimination[18]
- collecting by a means that would constitute a civil wrong, for example, by trespassing on private property or threatening damage to a person unless information is provided
- collecting information contrary to a court or tribunal order, for example, contrary to an injunction issued against the collector.

Collecting by fair means

3.62 A 'fair means' of collecting information is one that does not involve intimidation or deception, and is not unreasonably intrusive.[19] Whether a collection uses unfair means will depend on the circumstances. For example, it would usually be unfair to collect personal information covertly without the knowledge of the individual. However, this may be a fair means of collection if undertaken in connection with a fraud investigation.

3.63 The following are given as examples of where a collection of personal information may be unfair (some may also be unlawful):

- collecting from a file dumped by accident on a street, or from an electronic device which is lost or left unattended
- collecting from an individual who is traumatised, in a state of shock or intoxicated
- collecting in a way that disrespects cultural differences
- misrepresenting the purpose or effect of collection, or the consequences for the individual of not providing the requested information
- collecting by telephoning an individual in the middle of the night

[16] For example, *Criminal Code Act 1995, Part 10.7*.
[17] For example, *Telecommunications (Interception) Act 1979* (Cth) s 7; *Surveillance Devices Act 2004* (Cth) s 14.
[18] See for example, the *Disability Discrimination Act 1992*, s 30 and the *Sex Discrimination Act 1984*, s 27.
[19] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 77.

- collecting by deception, for example, wrongly claiming to be a police officer, doctor or trusted organisation.

Collecting directly from the individual

3.64 APP 3.6 provides that an APP entity 'must collect personal information about an individual only from the individual', unless one of the following exceptions apply:

- for all APP entities, it is unreasonable or impracticable for the entity to collect personal information only from the individual
- for agencies, the individual consents to the personal information being collected from someone other than the individual
- for agencies, the agency is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual.

Unreasonable or impracticable to collect directly from the individual

3.65 Whether it is 'unreasonable or impracticable' to collect personal information only from the individual concerned will depend on the circumstances of the particular case. Considerations that may be relevant include:

- whether the individual would reasonably expect personal information about them to be collected directly from them or from another source
- the sensitivity of the personal information being collected
- whether direct collection would jeopardise the purpose of collection or the integrity of the personal information collected
- any privacy risk if the information is collected from another source
- the time and cost involved of collecting directly from the individual. However, an APP entity is not excused from collecting from the individual rather than another source by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable or impracticable will depend on whether the burden is excessive in all the circumstances.

3.66 The following are given as examples of when it may be unreasonable or impracticable to collect personal information only from the individual concerned:

- collection by a law enforcement agency of personal information about an individual who is under investigation, where the collection may jeopardise the investigation if the personal information is collected only from that individual[20]
- if a legal or official document that is mailed to an individual is returned to the sender, the individual's current contact details may need to be obtained from another source.

[20] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 77.

Consent by the individual — for agencies only

3.67 The term 'consent' is discussed at paragraph 3.23 above and in Chapter B (Key concepts). As noted in those sections, consent can be express or implied, and must be voluntary, informed, current and specific, and the individual must have capacity to consent.

3.68 An example of where an agency might collect personal information from someone other than the individual is where an individual consents to one agency disclosing their personal information (such as contact details) to the other agency.

Required or authorised by law or a court or tribunal order — for agencies only

3.69 The meaning of 'required or authorised by or under an Australian law or a court/tribunal order' is discussed in Chapter B (Key concepts). It is a common feature of legislation that an agency, for the purpose of performing a function or exercising a power, is authorised to require a person or body to provide personal information.

3.70 An example of where collection by an agency from someone other than the individual concerned might be required or authorised by law is s 44 of the Privacy Act, which provides that the Information Commissioner may issue a notice to a person requiring them to provide specified information for the purpose of an investigation under the Act (and that information may include personal information).

Collecting personal information from a related body corporate

3.71 Section 13B(1)(a) provides that the collection of personal information about an individual (other than sensitive information) by a body corporate from a related body corporate is generally not 'an interference with the privacy of an individual' (interferences with privacy are discussed in Chapter A (Introductory matters)). This provision applies to collection of information from related bodies corporate and not to other corporate relationships such as a franchise or joint-venture relationship.[21]

3.72 The effect of s 13B(1)(a) is that an APP entity may collect personal information (other than sensitive information) from a related body corporate without satisfying the requirements of APP 3.1 or 3.2 (see paragraphs 3.8–3.21 above). However, s 13B(1A) sets out some exceptions to this, including where the related body corporate is not an organisation.

[21] Section 6(8) states 'for the purposes of this Act, the question of whether bodies corporate are related to each other is determined in the manner in which that question is determined under the *Corporations Act 2001*'.