



Australian Government

Office of the Australian Information Commissioner

May 2017

What is personal information?

Contents

Introduction	3
How does the Privacy Act define ‘personal information’?	4
Types of personal information	4
How can you determine whether information is ‘personal information’?	6
Can information have more than one subject matter?	12
Can personal information be about more than one person?	12
Does personal information have to be in a particular format?	13
What is <i>not</i> personal information?	14
Information that cannot identify an individual	14
Information that is not ‘about’ an individual	14
Business information	14
Information about deceased persons	15
De-identified information.....	15
Checklist for determining whether information is personal information	17
More information	17

Introduction

This resource aims to assist entities bound by the *Privacy Act 1988* (the Privacy Act) to understand and apply the definition of ‘personal information’ in section 6(1) of the Act. This resource should be read together with the Australian Privacy Principle (APP) guidelines.¹

The concept of ‘personal information’ is broad, and in most cases, whether or not information is personal information will be a straightforward question. However, in some cases it may not be as clear, and the answer will depend on the context and circumstances.

Where there is uncertainty, the Office of the Australian Information Commissioner (OAIC) encourages entities to err on the side of caution by treating the information as personal information, and handle it in accordance with the Australian Privacy Principles (APPs).

This guidance aims to take you through the factors that you may wish to consider when determining whether information is personal information. The examples are provided for illustrative purposes only.

¹ Available at <<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/>>.

How does the Privacy Act define 'personal information'?

The Privacy Act defines 'personal information' as:

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

The definition is technologically neutral to ensure sufficient flexibility to encompass changes in information-handling practices over time. It is also consistent with international standards and precedents.²

Types of personal information

The term 'personal information' encompasses a broad range of information.

A number of different types of information are explicitly recognised as constituting personal information under the Privacy Act. For example, the following are all types of personal information:

- 'sensitive information' (includes information or opinion about an individual's racial or ethnic origin, political opinion, religious beliefs, sexual orientation or criminal record, provided the information or opinion otherwise meets the definition of personal information)³
- 'health information' (which is also 'sensitive information')⁴
- 'credit information'⁵
- 'employee record' information (subject to exemptions⁶), and
- 'tax file number information'.⁷

Although not explicitly recognised as personal information under the Privacy Act, information may be explicitly recognised as personal information under other legislation. For example, under the *Telecommunications (Interceptions and Access) Act 1979* (Cth), certain telecommunications data

² Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 53.

³ See section 6(1) of the Privacy Act.

⁴ Ibid. See also the OAIC [Privacy Fact Sheet 49: Health information and your privacy](#).

⁵ See section 6N of the Privacy Act. Credit information is also personal information, however it is regulated separately under Part IIIA of the Privacy Act. See OAIC's 15 privacy fact sheets (26 to 40) on how personal information can be handled in the Australian consumer credit reporting system, available at <www.oaic.gov.au/individuals/privacy-fact-sheets/credit-reporting/>.

⁶ However, note that there is an 'employee record exemption' for some organisations. See section 6 of the Privacy Act, and the OAIC's [Privacy business resource 13: Application of the Australian Privacy Principles to the private sector](#).

⁷ See section 6(1) of the Privacy Act, and more generally the *Privacy (Tax File Number Rule) 2015*.

(sometimes referred to as ‘metadata’⁸) is taken to be personal information for the purposes of the Privacy Act.

However, information does not have to be explicitly recognised as personal information to constitute personal information under the Privacy Act. The types of information that are personal information are unlimited and can vary widely.

Further, the definition of personal information is not limited to information about an individual’s private or family life, but extends to any information or opinion that is about the individual, from which they are reasonably identifiable. This can include information about an individual’s business or work activities.

Personal information can range from sensitive and confidential information to information that is publicly available. The definition also makes clear that information will be personal information even if it is incorrect.⁹

Common examples of personal information

1. Information about a person’s private or family life

- A person’s name, signature, home address, email address, telephone number, date of birth, medical records, bank account details and employment details will generally constitute personal information.¹⁰

2. Information about a person’s working habits and practices

- A person’s employment details, such as work address and contact details, salary, job title and work practices.
- Certain business information — for example, information about a loan taken out by a sole trader to purchase tools for their business, or information about utility usage — may be personal information about the sole trader.¹¹

3. Commentary or opinion about a person

- In certain circumstances, a referee’s comments about a job applicant’s career, performance, attitudes and aptitude is ‘personal information’ as it is information about that person.¹² The referee’s comments may also be personal information about the referee given that they provide information about the referee’s views on a particular subject. Likewise, a trustee’s opinion about a bankrupt’s affairs and conduct can be personal information about both the bankrupt and the trustee.

⁸ Such metadata for the purposes of the *Telecommunications (Interceptions and Access) Act 1979* includes subscriber and account details for telecommunications services and devices; information about the sources and destinations of communications; the date, time and duration of communications; and the location of equipment or line used in connection with a communication (s 187AA).

⁹ In this regard, the APPs provide an opportunity to request access to an individual’s own personal information (APP 12) and a process for seeking corrections to personal information (APP 13).

¹⁰ Provided that the person is reasonably identifiable from the information in the relevant context in which it is used, or when considered together with other available information. For further information on when an individual is ‘reasonably identifiable’, see the relevant section below.

¹¹ However, for information to be personal information, it must be about a natural person (not a corporation).

¹² See also the definition of ‘employee record’ in section 6 of the Privacy Act.

- An opinion about an individual's attributes that is based on other information about them, such as an opinion formed about an individual's gender and ethnicity, based on information such as their name or their appearance. This will be personal information about the individual even if it is not correct.
- Information or opinion inferred about an individual from their activities, such as their tastes and preferences from online purchases they have made using a credit card, or from their web browsing history.

How can you determine whether information is 'personal information'?

For information to be personal information, it must be:

1. **about an identified individual; or**
2. **about an individual who is reasonably identifiable.**

It is important to remember that decisions about whether information is personal information should be made on a case-by-case basis, with reference to the circumstances and specific context of the situation.

Some information may not be personal information when considered on its own. However, when combined with other information held by (or accessible to) an entity, it may become 'personal information'. Information holdings can therefore be dynamic, and the character of information can change over time.

1. When is information 'about' an identified individual or an individual who is reasonably identifiable?

Information is 'about' an individual where there is a connection between the information and the individual.¹³ This is ultimately a question of fact, and will depend on the context and the circumstances of each particular case.

For example, information will be 'about' someone where the person is a subject matter of the information or opinion. It is important to remember that information can have multiple subject matters - so in many cases this will not be difficult to establish.¹⁴

Example one: Jane's name, phone number and email address are collected by a business or government agency to create a customer contact file. Jane's customer contact file constitutes personal information, as she is the subject of the record.

¹³ See *Telstra Corporation Limited and Privacy Commissioner* [2015] AATA 991 (18 December 2015) at [112], and *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 (19 January 2017), at [43] and [64] per Kenny and Edelman JJ.

¹⁴ See *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 (19 January 2017) at [63]-[64] per Kenny and Edelman JJ.

Example two: A private school publishes an article in a newsletter about a local sporting event, which includes information about the performance of various students, including Bob and Lisa. As Bob and Lisa are (two of the many) subjects of the article, the article contains their personal information.

Information will also be ‘about’ someone where it reveals or conveys something about them — even where the person may not, at first, appear to be a subject matter of the information.

Example one: Kim’s agency client number (but not his name) appears in a list of benefit recipients. As the inclusion of his client number in this list reveals that he is the recipient of a benefit, this would be Kim’s personal information (assuming Kim is also reasonably identifiable from his client number – see section below). For the agency, there is a clear connection between the client number and Kim.

Example two: Information that Sue was born with foetal alcohol syndrome reveals that her biological mother consumed alcohol during her pregnancy. This information may therefore be personal information about Sue’s mother as well as Sue.

Example three: Miro’s car breaks down and he lodges an insurance claim. His insurance company employs an independent investigator to examine the car and determine the cause of the breakdown. The investigator’s report addresses a number of mechanical issues, and includes a conclusion that ‘the owner has contributed to the breakdown by driving negligently’. While the investigator’s report does not name or refer to Miro personally — and the main subject of the report appears to be Miro’s car — the investigator’s opinion also conveys something about Miro. Namely, an opinion that Miro has driven the car in a particular way. Parts of the investigator’s report may therefore be about Miro as well as the car. Provided Miro is reasonably identifiable from the information in the report (see below), it may constitute his personal information.

Information can have different degrees of connection with an individual and still be personal information. However, at some point, the connection between the information and a person will be too remote for the information to be personal information.¹⁵

¹⁵ Ibid at [64], and see *Telstra Corporation Limited and Privacy Commissioner* [2015] AATA 991 (18 December 2015) at [43]. See examples below in the section ‘What is not personal information’.

2. When does information identify or reasonably identify an individual?

When will information be about an ‘identified’ individual?

Generally speaking, an individual is ‘identified’ when, within a group of persons, he or she is ‘distinguished’ from all other members of a group. For the purposes of the Privacy Act, this will be achieved through establishing a link between information and a particular person.

This may not necessarily involve identifying the individual by name. Even if a name is not present other information, such as a photograph or a detailed description, may also identify an individual. The key factor to consider is whether the information can be linked back to the specific person that it relates to.

Example one: By itself, information that allows Nina to be contacted — such as a telephone number or a street address — may not be about an ‘identifiable’ individual. However, Nina is likely to be identified where this information can be used to search a business’s customer database, locating an entry about Nina.

Example two: Information is included on Michael’s medical record about his biological father, Mario. Therefore, the information on Michael’s medical record may be Mario’s personal information as well - even where Mario’s name is not included (because there is only one individual who is Michael’s biological father).

When is an individual ‘reasonably identifiable’?

This answer to this question will depend on the relevant context the information is being handled in. Certain information may be unique to a particular individual, and therefore may (in and of itself) establish a link to the particular person. However, for an individual to be ‘identifiable’, they do not necessarily need to be identified from the specific information being handled. An individual can be ‘identifiable’ where the information is able to be linked with other information that could ultimately identify the individual.

The inclusion of the term ‘reasonably’ in the definition of personal information means that where it is possible to identify an individual from available information, the next consideration is whether the process of identification is reasonable to achieve. This is determined by asking whether, objectively speaking, it is reasonable to expect that the subject of the information could be identified. 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 of it occurring, the information would not generally be regarded as ‘personal information’.

Determining whether a person is ‘reasonably’ identifiable will require a contextual consideration of the particular circumstances, including:

- a) the nature and amount of information
- b) who will hold and have access to the information, and
- c) the other information that is available, and the practicability of using that information to identify an individual.

a) The nature and amount of information

The more information about an individual that an entity holds or to which it has access, the more likely it is that the person will be reasonably identifiable from that information. Likewise, some information that is specific to an individual will more readily identify that individual than other types of information that are of a more general nature.

Example one: If an entity holds only one item of information about Sylvia, such as her first name, it might not be possible to identify her just from that information. However, if the entity holds additional information about Sylvia, such as her age, gender, postcode and occupation, it becomes increasingly likely that the entity will be able to identify her.

Example two: Esther has a unique tattoo. A description of Esther's tattoo may more readily identify her than a description of a very common tattoo.

b) Who will hold and have access to the information

Whether or not an individual is reasonably identifiable from information will also be influenced by who holds and has access to information. Information that enables an individual to be identified in one context may not identify the individual in a different context. In particular, the likelihood of identification will usually be higher where the subject is known to the person who has access to the information.

Generally speaking, where information is publicly released, entities should be aware that the information could be accessed by anyone in the world. This may make it difficult to anticipate who might access the information, what other types of information they may have access to for referencing purposes, and what motivations they may have to identify an individual. This is why it is crucial that information which may be personal information is handled carefully and securely.

Example one: A law enforcement agency with access to a car registration database might be able to use a licence plate number to identify that Mark is the registered owner of a particular car. However, an average member of the public would be less likely to be able to use this information to identify Mark as the registered owner. Accordingly, Mark's licence plate number may be 'personal information' when held by or disclosed to an employee of a law enforcement agency, but may not be personal information in the hands of an average member of the public.

Example two: John Smith, a private school student, has a very common first and family name. His first and/or last name would likely identify him in his classroom and possibly at his school. However, it is less likely that John's name could enable him to be identified out of the entire population of private school students in Australia.

c) The other information that is available (or known) to the recipient, and the practicability of using that information to identify an individual

Some information is unique to a particular person, and may in and of itself identify that person. However, for a person to be reasonably identifiable, it is not necessary that they are reasonably identifiable solely from the information in question. Whether a person is 'reasonably identifiable' will be influenced by whether the entity that holds the information can identify the individual by referencing it with other available information (and in some cases, whether the entity/person who holds the information already knows certain information about the person). This includes use of other information held by (or available to) that entity, and any publically available information.

Where it is technically possible to identify an individual by referencing it against other available information, entities should also consider the likelihood that this would occur. The time (and in some cases, the cost) that would be involved in identifying the person, and the resources and operational capacity of the entity that holds the information, all contribute to the likelihood that identification would occur. For example, an individual is more likely to be reasonably identifiable from information held by an entity when the entity's staff have access to, or can easily obtain, other information about the individual. By contrast, where the process of identifying the individual is so impractical that there is almost no likelihood of it occurring, the available information would not generally be regarded as 'reasonably' identifying the individual.

As part of assessing the likelihood of identification, entities should also consider whether an entity (or a particular person) may be especially motivated to attempt to identify someone. For example, there may be individuals who are highly motivated to identify persons living in a particular domestic violence refuge.

The feasibility of a particular method of identifying an individual can change with new developments in technology and security, or changes to the public availability of certain records. If an entity has decided that the information it holds does not allow the identification of individuals, that decision should be reviewed regularly in light of any such developments.

Example one: Ava, Betty, Charles, Dino and Edward are the top five runners in a fun run. A list of the running times of all participants in the fun run, by itself, would not necessarily reveal their identity. However, if the running times were able to be cross-matched with other information (such as a list naming the top five fastest runners) then in these circumstances, the list of running times may be personal information about these five people.

Example two: As part of its customer loyalty program, a company holds identifying information about each of its members as well as other information (for example, about each member's transactions). The company wants to conduct data analytics on this information, so it removes some of the identifying details (for example name, address, date of birth, contact numbers) and instead assigns each customer file a unique customer identifier. The customer files are then given to a third party data analytics company for research purposes. In the hands of the third party data analytics company, this information may not be personal information. However, if employees within the company are reasonably able to match the unique identifier with the original customer record to identify the person, this information would be personal information when handled by the company.

Real-life case studies

Case study one: In 2000, a university student used publicly available health insurance information on workers employed by the state of Massachusetts. The information had the names, addresses, social security numbers and some other 'identifying' information of the workers removed. The researchers obtained the state voter rolls for the capital city of Cambridge. These provided the name, postcode, address, sex and date of birth of every registrant. The insurance data revealed that there were six people in the city of Cambridge who were born on the same day as the State Governor. Half of those were men. The voter data allowed the researchers to pinpoint the Governor as the only one of those persons living in a particular postcode in Cambridge. The corresponding health-insurance data revealed the Governor's health information, including medical diagnoses and prescriptions.¹⁶

Case study two: In 2006, AOL, a search engine provider, released apparently anonymous web search records for 658,000 users. However, some journalists working for the New York Times were able to link the search terms to identify users and contacted them. For example, 'Subscriber 4417749' was able to be identified as a 62-year old woman, through her searches for local real estate agents and gardeners, her use of dating sites, health queries she had entered about her 'numb fingers' and questions about her dog's behaviour.¹⁷

¹⁶ Paul Ohm, 2010, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', *UCLA Law Review*, Vol. 57, p. 1701.

¹⁷ Michael Barbaro and Tom Zeller Jr, 2006, 'A Face is Exposed for AOL Searcher No. 4417749', *New York Times* <<http://www.nytimes.com/2006/08/09/technology/09aol.html>>.

Can information have more than one subject matter?

Yes. Information that is about something other than an individual — a car, for example, or a piece of land — can still be about an individual as well. The key question to consider is whether the individual is a subject of the information, and/or the information reveals or conveys something about that person.

Example one: Information that the body corporate fees for Xavier's property have not been paid for a year is about the property, but it also reveals a fact about Xavier — that he has not paid his body corporate fees owed to the strata manager. This would therefore still be personal information about Xavier, even though the information may appear to be primarily about the property. Further, there is a clear connection between Xavier and the property, given that he is the property owner.

Example two: Information collected by an insurance company about a car being parked at a certain address overnight on a regular basis is about the car. However, particularly when combined with other information, this fact about the car may also reveal that Zoe, the car's owner, knows someone at that address and spends time there regularly. This means that the information about the car may also be personal information about Zoe.

Can personal information be about more than one person?

Personal information of one individual can also be the personal information of another person or persons. This is known as 'joint personal information.'

Example one: Information provided for a joint loan application contains personal information about both parties to the loan application.

Example two: A file note made by a doctor about his or her opinion about a patient's prognosis contains personal information about the patient, but the opinion may also be the personal information of the doctor giving it.

Does personal information have to be in a particular format?

Personal information can be in any format – it is not limited to information that is contained in records.¹⁸ The definition expressly states that information is personal information ‘whether the information or opinion is recorded in a material form or not’.

Personal information can include information that is:

- shared verbally
- captured digitally
- recorded
- captured on signs.

For example, some personal information does not contain any words at all, such as images (especially photos) and sounds (voice or tape recordings) — or can be latent in a material item (for example, DNA in human tissue).

Example one: A telecommunications company records the phone calls that are received by its enquiries line. A recording of a call which contains an individual’s voice may be that individual’s personal information where the recorded person is reasonably identifiable. For example, where the recording is contained within or linked to the customer’s file. (**Note:** this will likely also be personal information of the employee who took the call, provided they are reasonably identifiable.)

Example two: Tagged photographs of a person posted on a social media site will usually constitute personal information.

¹⁸ We note that some of the APP obligations, for example APP 6, only apply to information held in a record.

What is *not* personal information?

Information that cannot identify an individual

Information that is not about an identified individual, or an individual who is reasonably identifiable, will not be personal information.

Example: An aerial photograph taken of an individual in front of the Sydney Opera House would be unlikely to constitute personal information as the photograph would not show enough detail to even be able to determine the person's gender or identifying features. However, a similar photo taken at a closer distance would be more likely to constitute personal information, for example, where the person's features and clothing are more clearly discernible.

Information that is not 'about' an individual

Information that is not 'about' an individual — because the connection with the person is too tenuous or remote - is not 'personal information'.

Example one: A government report which states that some yet to be specifically identified land in a general locality may be subject to compulsory acquisition in the future would not be personal information — as the possibility of compulsory acquisition does not establish a sufficient connection with particular owners of land in the locality.

Example two: In contrast, the federal government announces that all the houses along a particular side of road X between street A and street B will be subject to compulsory acquisition, in order to build a new airport. This may be considered personal information about the owners of the specified land, because it reveals those particular individuals will lose their land.

Business information

Generally, information that is only about a business is not considered to be 'personal information'. This is because the Privacy Act defines an 'individual' as a 'natural person', and the ordinary meaning of a 'natural person' does not include a body politic or corporate entity (including a company).

However, an individual's personal information may be so interconnected to information about his or her business or company that information about that business or company can constitute personal information about the individual. For instance, where the business is owned and managed by a sole trader, the distinction between business information and personal information might sometimes overlap.

In practice, where information provided in a business or professional capacity is also personal information, the APPs will apply.

Example: Information about the utility bills paid by a publically listed company over the last year would not be personal information, as this information would not identify an individual.

Information about deceased persons

In most cases, information about deceased persons is not considered to be ‘personal information’. Personal information is information about an individual, which means a natural person and does not include a deceased person. However, if information about a deceased person includes information or an opinion about a living individual, it will be ‘personal information’ about that ‘living individual’.

Example: Jonathan’s death certificate contains information about his next of kin, including his wife, Margaret, and daughter, Eliza. While the information about Jonathan contained in the certificate would not be personal information, if Margaret and Eliza are reasonably identifiable, then the information included about them on the death certificate would be personal information.

De-identified information

De-identified information is not ‘personal information’, as it is no longer about an identifiable individual or an individual who is reasonably identifiable (see the definition of ‘de-identified’ in s 6(1) of the Privacy Act).

De-identification is a process which involves the removal or alteration of information that identifies a person or is reasonably likely to identify them, as well as the application of any additional protections required to prevent identification. This will generally require a number of steps, including:

- the removal or alteration of personal identifiers (such as name, address, date or birth, and other identifying information), and
- the application of any additional techniques required to obscure, aggregate, alter and/or protect the data in some way so that it no longer allows any individuals to be reasonably identified.

The OAIC encourages entities to seek specialist advice when de-identifying information, to ensure that the most appropriate techniques are used.¹⁹ In addition to techniques applied to the data itself, restrictions on the data environment (for example, imposing restrictions on how and where the data may be accessed and requiring that data users sign non-disclosure agreements) may also be necessary to help ensure that no individuals are identifiable or reasonably identifiable.

¹⁹ The OAIC is currently revising its de-identification guidance, and plans to issue this in the near future. See also the OAIC’s existing [Privacy business resource 4: De-identification of data and information](#).

It can be difficult to determine whether information has been successfully de-identified. To be considered 'de-identified' for the purposes of the Privacy Act, the information must have a very low risk of re-identification, having regard to all the circumstances (and in particular, the context in which the information will be handled, including who will have access to the data, and what other information they might have access to). Any information which is re-identified from an apparently de-identified dataset will be personal information, and must therefore be handled in accordance with the Privacy Act.

Whether information is de-identified is heavily context dependent. Information might be considered to be personal information in one context, but not in another. For instance, if de-identified information is disclosed to an entity which is legally obliged to take steps to ensure that it is not re-identified (and it does take such steps), then in the hands of that entity, the information might not be personal information. By contrast, if the same information was to be publically released, there would likely be a much higher likelihood of re-identification because anyone in the world could access that information.

Example: Where a research organisation is under strict contractual obligations to ensure that information in a specific dataset is not re-identified — for example, by ensuring data is accessed only by researchers in a secure computer lab environment, where access to external materials (for example, via the internet) is not possible — the information might be de-identified in that context. If, however the same data was to be made freely available on a website, it would likely be personal information as the data subjects may be reasonably identifiable.

Checklist for determining whether information is personal information

Information will be personal information where it is about an identified or reasonably identifiable individual. Information may not, by itself, be personal information. However, in combination with other information, it may be.

To assist in determining whether information is personal information, consider the following questions:

- Is the information ‘about’ an individual – that is, is there a connection between the information and the person? This is a question of fact, and depends on the context and circumstances.
 - Some information is clearly about an individual – for example, name, date of birth, occupation details, medical records.
 - Otherwise — does the information reveal a fact or opinion about the person, in a way that is not too tenuous or remote?
- Is the relevant individual identified, or reasonably identifiable? Entities should consider all relevant contextual factors, including:
 - the nature and amount of information
 - who will have access to the information
 - other information that is available.
- **Remember** — when in doubt, err on the side of caution and treat the information as personal information.

More information

The following resources may also assist APP entities to understand and comply with the requirements in the Privacy Act:

- [Fact sheet 17 — Australian Privacy Principles](#), which provides the text of the 13 APPs.
- [Australian Privacy Principles guidelines](#) for more information about interpreting and applying the APPs.
- [Privacy business resource 4: De-identification of data and information](#)

The examples provided in this resource are for illustrative purposes only. APP entities will need to consider how the Privacy Act applies to their particular situation.