Australian Government
Office of the Australian Information Commissioner

Guide to big data and the Australian Privacy Principles

Consultation draft

May 2016

Contents

Foreword

Big data analytics has changed the way we identify trends and challenges, as well as identify opportunities. This means big data has the potential to bring about enormous social and economic benefits.

The Office of the Australian Information Commissioner has developed the draft *Guide to big data and the Australian Privacy Principles* to facilitate big data activities while protecting personal information.

Many big data privacy challenges are addressed in this guide, including notice and consent, collection and retention minimisation, as well as use limitation.

The draft Guide outlines key privacy requirements and encourages the implementation of the Privacy Management Framework. Taking this approach will embed 'privacy by design' in entities' culture, systems and initiatives from the design stage onwards.

The guide is intended for use by entities covered by the *Privacy Act 1988*. It may also be useful as a model for better personal information handling practice for organisations not subject to the Privacy Act.

We welcome your feedback on the draft guide.

Timothy Pilgrim

Acting Australian Information Commissioner

Introduction

This *Guide to big data and the Australian Privacy Principles* (the guide) provides guidance about the Australian Privacy Principles (APPs) and how they apply to big data.

The guide should be read in conjunction with the *Australian Privacy Principles guidelines* (APP guidelines) which outline the mandatory requirements of the APPs and how the Office of the Australian Information Commissioner (OAIC) interprets the APPs, together with guidance for best practice.

The term 'big data activities' is used in this guide. Big data activities include big data analytics, as well as the handling of personal information before and after analysis. This includes how personal information is managed, collected, dealt with and maintained.

The guide is intended for use by entities covered by the *Privacy Act 1988 (Cth)* (Privacy Act), including organisations, agencies, credit reporting bodies, credit providers and tax file number recipients.[1] The guidance provided will also be useful for entities undertaking traditional data matching[2] and data aggregation activities.

This guide is not legally binding. The OAIC will however refer to this guide when undertaking its functions under the Privacy Act. The *OAIC's Privacy regulatory action policy* provides information on when and how we may exercise our functions.

This guide assumes some knowledge of privacy concepts.

What is big data?

Big data has come about from a fundamental shift in analytical processes, together with large data sets, increased computational power and storage capacity. There is no definitive definition for big data. Gartner's 'three Vs' definition is however often used:

> […]high-*volume*, high-*velocity* and/or high-*variety* information assets that demand cost-effective, innovative forms of information processing for enhanced insight, decision making, and process optimization.[3]

Big data analytics has changed the way entities use data to identify trends and challenges, by analysing large date sets, often from a variety of sources, quickly. The data sets are analysed by applying algorithms to find correlations. This is different to how data was analysed in the past where particular hypotheses were tested.

[1] For more information on the jurisdiction of the Privacy Act, see our 'Privacy Act' webpage, see: www.oaic.gov.au/privacy-law/privacy-act.

[2] For more information about the requirements for data matching in Australian government see: www.oaic.gov.au/privacy-law/other-legislation/government-data-matching.

[3] Gartner, *The Importance of 'Big data': A Definition*, cited in Department of Finance and Deregulation, *The Australian Public Service Big Data Strategy*, 2013, p 8, see: http://www.finance.gov.au/sites/default/files/Big-Data-Strategy.pdf.

Big data and privacy

Data used for big data analytics may include personal information. Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.[4]

The Privacy Act regulates how entities handle personal information, including sensitive information. The Act includes the APPs which set out standards, rights and obligations in relation to handling, holding, accessing and correcting personal information.

The application of the APPs to big data is discussed in this guide.

De-identified personal information

Entities considering undertaking big data activities should first consider whether de-identified personal information could be utilised.

Personal information may be de-identified so that the information is no longer about an identifiable individual or an individual who is reasonably identifiable (s 6(1)). Data that has been successfully de-identified is not personal information.[5]

De-identifying personal information for the purposes of big data activities means the information may be used, shared and published without jeopardising personal privacy. This enables organisations to maximise the utility and value of the information while safeguarding privacy. De-identifying information also lessens the risk that personal information will be compromised should a data breach occur.

There are a number of points during a big data activity when de-identification may occur. For example, de-identification may occur when the personal information is collected, prior to it being used for big data analytics, or before the analytical outcomes are presented.

Privacy tip: Successfully de-identified data is not personal information meaning the Privacy Act will generally not apply.[6]

De-identifying personal information

Guidance about de-identifying personal information is provided in Privacy business resource 4: De-identification of data and information and Information policy agency resource 1: De-identification of data and information. These resources provide guidance

[4] See Privacy Act s (6)(1). For a more detailed explanation, see: www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-b-key-concepts.

[5] Note: Credit reporting bodies must also comply with section 20M of the Privacy Act which prevents the use and disclosure of de-identified credit reporting information except when that use or disclosure is for the purpose of conducting research in accordance with the *Privacy (Credit Related Research) Rule 2014*, https://www.comlaw.gov.au/Details/F2014L00503.

[6] As above.

about whether de-identification may be appropriate, choosing de-identification techniques and assessing the risk of re-identification.

For the purposes of big data, entities considering de-identifying personal information should undertake a risk assessment. This could be undertaken as part of a Privacy impact assessment (PIA) for the proposed big data activity.

A risk assessment should consider the nature of the personal information, the de-identification techniques that may be used and the context in which the de-identified information will be handled. For example, whether it will be used for big data activities within the entity, or whether the de-identified data will be disclosed to another entity for this purpose.

Privacy impact assessments

Privacy impact assessments (PIA) should be used when an entity is developing or reviewing a project that uses big data. PIAs are practical tools which facilitate 'privacy by design' because they encourage entities to develop projects with privacy designed into the project, rather than being bolted on afterwards.

A PIA identifies how a project can impact an individual's privacy and makes recommendations for managing, minimising or eliminating privacy impacts. The OAIC recommends that entities conduct PIAs as part of their regular risk management and planning processes.

Undertaking PIAs for big data activities will help entities describe their aims and the key privacy impacts for the activity. For example, a PIA may explain the insights an entity may obtain from undertaking a big data activity and how the data will be sourced and managed for the activity. It could also consider whether using de-identified information would be appropriate.

Where an entity collects data for a particular purpose and the big data activity would use the data for another purpose (known as a 'secondary purpose') the PIA might explore how this might be done and how the privacy impacts will be addressed.

More information about undertaking a PIA is provided in the Guide to undertaking privacy impact assessments.

Re-identification of personal information

Where an entity is proposing to de-identify personal information for a big data activity they should undertake a risk assessment to consider the risk of re-identification and collection of personal information during or following big data activities (collection of personal information is discussed below). In undertaking a risk assessment entities should consider the variety of information that will be brought together, the algorithms to be applied, and how the outcomes will be used or disclosed.

For example, where the de-identified information will be made available to other entities or the public generally, the relevant factors to consider may include the cost, difficulty, practicality and likelihood that the information may be re-identified.

Following a risk assessment, appropriate mitigation strategies should be implemented. This may include using different or additional de-identification techniques. It may also include placing restrictions on the use of the de-identified information.

Where personal information is appropriately de-identified and mitigation strategies are implemented, the risk of re-identification should be low. If, however, personal information is re-identified during big data activities the Privacy Act regulates how it is to be handled, managed, dealt with and maintained.

Risk point: Where de-identification is not done properly, big data activities may lead to re-identification of personal information.

Privacy tip: Undertake a risk assessment to consider the likelihood of re-identification. Use appropriate de-identification techniques and implement risk mitigation strategies.

Australian Privacy Principles and big data

Big data challenges how key privacy principles, including notice and consent, data collection and retention minimisation, as well as use limitation, work in practice. The APPs are, however, technologically neutral and principles-based. This means entities have the flexibility to tailor their personal information handling practices for big data.

The APPs are structured to reflect the information lifecycle. This includes:

- considering the management of personal information (APP 1)
- notice and collection of personal information (APPs 3 and 5)
- dealing with personal information (APPs 6, 7 and 8), and
- maintaining personal information (APPs 10 and 11).

The requirements in each of these principles interact with and complement each other.

Management of personal information

The object of APP 1 is 'to ensure that entities manage personal information in an open and transparent way'. This enhances the accountability of entities' personal information handling practices, which in turn can build community trust and confidence.

APP 1 lays down the first step in the information lifecycle – planning, and explaining how personal information will be handled before it is collected. In practice, entities may comply with APP 1 by implementing the Privacy Management Framework and adopting a 'privacy by design' approach to big data.

Privacy by design

'Privacy by design' is a holistic approach where privacy is integrated and embedded in an entity's culture, practices and processes, systems and initiatives from the design stage onwards.[7]

In practice, this means entities should embed 'privacy by design' across and within their organisation, as well as for individual projects and activities. This includes taking a risk management approach to identifying privacy risks and mitigating those risks from occurring.

Embedding 'privacy by design' will lead to a trickle down effect where privacy is considered automatically by the entity, resulting in better overall privacy practice and compliance.

Using the Privacy Management Framework in the big data context

Entities that undertake big data activities should implement the four steps outlined in the Privacy Management Framework. This starts with being open and transparent about how they will handle personal information for big data.

Step 1: Embed: a culture of privacy that enables compliance

Entities should ensure their leadership and governance arrangements create a culture of privacy that values personal information. This may include:

- appointing a key privacy officer to be responsible for managing and reporting privacy issues, including for big data
- outlining in strategic documents how data sets containing personal information are treated as valuable assets for big data, and how they are managed and protected
- developing and implementing a privacy management plan that outlines how big data activities align with the entity's privacy obligations on an ongoing basis.

Step 2: Establish: robust and effective privacy practices, procedures and systems

Entities are required to take reasonable steps to implement practices, procedures and systems that ensure compliance with the APPs, and enable the entity to deal with privacy related enquiries and complaints from individuals.

Entities should take a risk management approach to identifying what reasonable steps to take to comply with APP 1.2. The size of the entity, its resources, the complexity of its operations and business model are all relevant to determining what steps are reasonable. Reasonable steps may include:

[7] More information about 'Privacy by design' is available from the Information and Privacy Commissioner of Ontario's website, see: www.ipc.on.ca/english/privacy/introduction-to-pbd/.

- committing to using 'privacy by design', including PIAs to inform big data activities
- developing policies and procedures for personal information used for big data activities that address the full lifecycle of that information (including an APP privacy policy)
- establishing clear policies, and APP 5 notices, (which are discussed below), regarding the secondary use of personal information for big data activities.

For example, an entity that regularly undertakes big data analytics as part of its business model will need to implement more rigorous and detailed procedures for big data than an entity that is provided trends and insights from big data analytics.

APP privacy policy

APP 1.3 requires entities to have clearly expressed and up-to-date privacy policies describing how they manage personal information. An APP privacy policy is a key tool for ensuring open and transparent management of personal information.

Entities should prepare and maintain an APP privacy policy as part of implementing the Privacy Management Framework. An APP privacy policy should describe the main functions and activities of an entity, and identify those that involve personal information handling.

Entities undertaking big data activities should include general information about those activities in their APP privacy policy. For example, by including that they undertake big data analytics for marketing or policy development.

More information about developing an APP privacy policy, including an APP privacy policy checklist, is provided in the Guide to developing an APP privacy policy.

Step 3: Evaluate: your privacy practices, procedures and systems to ensure continued effectiveness

Entities should systematically examine the effectiveness and appropriateness of the privacy practices, procedures and systems to ensure they remain effective and appropriate. Lessons learned from big data activities, privacy complaints and breaches, as well as customer feedback can be used by entities to effectively undertake this step.

Step 4: Enhance: your response to privacy issues

Good privacy management requires entities to be proactive, forward thinking and to anticipate future challenges. By continually improving privacy processes, entities will ensure they are responsive to new privacy issues and that implementing improvements will not be a burden.

In undertaking Step 4, entities may:

- use the results of Step 3 evaluations to make necessary and appropriate changes to the entity's practices, procedures and systems

- consider having a big data activity externally assessed to identify areas where privacy processes may be improved
- continuously monitor and address new security risks and threats to data held.

More information about implementing the Privacy Management Framework is provided in Privacy Management Framework: enabling compliance and encouraging good practice.

Collection and notice

Personal information collected by an entity may only be used or disclosed for the primary purpose for which it was collected, unless an exception applies. This means the way personal information is collected, and the notice given to the individual concerned, is important for big data activities.

Entities should implement the Privacy Management Framework, which incorporates 'privacy by design' and encourages the use of PIAs, to inform their big data activities. This includes mapping the information lifecycle, identifying what personal information is collected, whether it might be utilised for big data and for what purpose. Undertaking these steps will inform what personal information should be collected, how it should be collected and what notice should be given.

The Privacy Management Framework is discussed above.

APP 3 – Collecting personal information

APP 3 provides when personal information, including sensitive information, may be solicited and collected by entities. It also provides that the collection of personal information must be by lawful and fair means. Unless it is unreasonable or impracticable, APP 3 also provides that personal information must be collected from the individual concerned.

Soliciting and collecting personal information

Agencies may only solicit and collect personal information that is reasonably necessary for, or directly related to, one or more of the agency's functions or activities (APP 3.1). Organisations may only solicit and collect personal information that is reasonably necessary for one or more of the organisation's functions or activities. (APP 3.2). Chapter 3 of the APP guidelines provides information on how to determine whether a particular collection of personal information is permitted.

APP 3 is intended to operate objectively and practically. This means that an entity may collect personal information that is reasonably necessary (from the point of view of a reasonable person) to pursue its legitimate functions or activities.

For big data, this requires entities to consider what personal information is reasonably necessary and for what purpose. This may appear to challenge the big data concept of using 'all the data' for 'unknown purposes'.

In practice however, entities continue to make decisions about what data to collect and use, including for their big data activities. The requirements of APP 3 mean that in making

those decisions, entities should consider what personal information is reasonably necessary for the entity's functions or activities. Complying with APP 3 will strengthen entities' business cases for proposed big data activities.

Risk point: Using 'all the data' for 'unknown purposes' will expose entities to privacy compliance risks.

Privacy tip: When entities are considering their business case for big data activities they should consider APP 3. A privacy impact assessment is a useful tool for this process.

Collecting personal information

The concept of 'collects' applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means. This includes collection by 'creation' which may occur when it is created or generated from other information the entity holds.

Big data analytics can lead to the creation of personal information. This can occur for example, when an entity uses a large variety of non-identifying information which it analyses, and in the process of analysing the information it becomes identified or reasonably identifiable. Similarly, insights about an identified individual from big data analytics may lead to the collection of new categories of personal information.

Where an entity collects personal information 'via creation' through big data analytics they need to consider whether they could have solicited and collected the personal information (APP 3.1 and 3.2). More information about collection is provided in Chapter 3 of the APP guidelines.

Risk point: Big data analytics may lead to the collection 'via creation' of personal information.

Privacy tip: Entities should undertake a privacy impact assessment which addresses whether personal information may be collected via creation through big data analytics.

Collection by lawful and fair means

An entity must collect personal information by lawful and fair means (APP 3.5). Collection that would not be lawful includes collecting in breach of legislation or contrary to a court order. While a 'fair means' of collecting information is one that does not involve intimidation or deception and is not unreasonably intrusive.

More information about collection is provided in Chapter 3 of the APP guidelines.

Collecting directly from the individual

Entities must collect personal information about an individual from the individual unless it is unreasonable or impracticable. While agencies may also collect personal information from someone other than the individual if the individual consents, or the agency is required or authorised by or under an Australian law, or a court/tribunal order to do so.

Whether it would be 'unreasonable or impracticable' may involve considering the sensitivity of the information collected and whether the individual would reasonably expect it to be collected from another source. More information about when it would be unreasonable or impracticable is provided in Chapter 3 of the APP guidelines.

In practice, personal information collected for big data activities will be from a variety of sources. Some will be collected directly from the individual, while some will be collected from other entities (that is, third parties).

Where an entity collects personal information from a third party, it should consider whether the third party's APP privacy policy and relevant APP 5 notices describe the circumstances in which the information will be disclosed.

It may be also be appropriate to have controls in place with third parties that govern the collection and disclosure of personal information. The notice the entity should provide in these circumstances is also discussed below.

Risk point: Personal information used in big data activities is likely to include information collected from third parties.

Privacy tip: Entities should undertake privacy impact assessments which consider how personal information will be collected for big data activities. This may include considering whether the exceptions to collecting directly from the individual are met and ensuring appropriate notice under APP 5 is provided.

Collecting sensitive information

Sensitive information is a subset of personal information that is generally afforded a higher level of privacy protection under the APPs. For example, sensitive information includes information about a person's political opinions, religious beliefs, sexual orientation and health information. The full definition of sensitive information is provided in the APP Guidelines.

Entities may only solicit and collect sensitive information if the individual consents to the collection, unless an exception applies, such as where the collection is authorised or required by law (the exceptions to collecting sensitive information are discussed in Chapter 3 of the APP guidelines). Consent is defined as 'express consent or implied consent' (s 6(1)). One exception to the requirement for consent to collecting sensitive information is where a permitted health situation exists.

Consent is discussed in more detail in Chapter B (Key concepts) of the APP guidelines.

Permitted health situation

The permitted health situation exception only applies to organisations. An example of a permitted health situation is where an organisation seeks to collect health information that is necessary for research relevant to public health or public safety, and the research purpose cannot be served by collecting de-identified information, and it is impracticable to obtain the individual's consent to collecting the health information.

In this situation, an organisation can collect health information provided that the collection is either required by law, or is in accordance with the guidelines approved by the Information Commissioner under s 95A of the Privacy Act (s 95A guidelines).[8]

An organisation seeking to rely on the s 95A guidelines must be satisfied that the research for which health information is to be collected has been approved by a Human Research Ethics Committee (HREC) in accordance with the guidelines. HRECs assess proposals to handle health information by organisations for health research (without individuals' consent). They may approve a proposed research activity where they determine that the public interest in the research activity substantially outweighs the public interest in the protection of privacy.

Guidance about using sensitive information collected on the basis of a permitted health situation is provided below.

The other exceptions to seeking the consent of the individual to collect sensitive information are discussed in Chapter 3 of the APP guidelines.

Risk point: Entities need the consent of the individual concerned to collect sensitive information (unless an exception applies).

Privacy tip: An entity should undertake a privacy impact assessment which considers whether sensitive information will be collected for the big data activity and on what basis.

APP 5 – Notification of collection of personal information

APP 5 requires an entity that collects personal information about an individual to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters. An entity must take reasonable steps before, at the time of collection, or as soon as practicable after it collects personal information.

An APP 5 privacy notice is different to an APP privacy policy. A privacy notice should provide specific information relevant to a particular collection of personal information. The purpose of the privacy notice is to provide an individual with enough relevant information to make an informed decision about whether to provide their personal information to an entity. While an APP privacy policy is more general in nature about the entity's information handling practices it should generally not be used as a substitute for an APP 5 privacy notice.

The APP 5 matters that need to be notified include 'the fact and circumstances of collection' and 'the purposes of collection' which can pose particular challenges for big data. Information about the other matters to be notified is provided in Chapter 5 of the APP guidelines.

[8] See s 16B(2) of the *Privacy Act 1988*.

The fact and circumstances of collection

Entities may include information about how, when and from where the personal information was collected. These details are particularly important when the entity collects the personal information:

- from a third party
- where the personal information is collected via creation
- where the individual may not be aware that their personal information was collected.

The purposes of collection

Entities may not use personal information for a purpose other than the primary purpose it was collected for unless an exception applies. Exceptions include where the individual has consented or the individual would reasonably expect the other use (see below for more information about using personal information). If an entity plans to use or disclose personal information for purposes other than the primary purpose (known as a 'secondary purpose') these should also be included in the privacy notice.

Big data activities will generally be a secondary use of personal information. This means privacy notices have an important role to play. Entities will need to provide adequate information about the collection and potential uses while ensuring the notice does not become overly vague or overly detailed.

Where multiple uses are included in a notice, entities should consider whether individuals have the opportunity to choose which collections, uses and disclosures they agree to and which they do not. PIAs are useful for informing the content of notices.

More information about the use of personal information, based on the notified purposes of collection, is provided below. While more information about the other specific matters that need to be notified is provided in Chapter 5 of the APP guidelines.

Risk point: Research shows many people don't read privacy notices.

Privacy tip: Entities should use privacy impact assessments to inform what information to include in their notices and then provide it in easy to read, dynamic and user centric ways.

Reasonable steps

An entity must take reasonable steps to notify an individual under APP 5 or ensure the individual is aware of the APP 5 matters. What are reasonable steps for an entity will depend upon circumstances including:

- the sensitivity of the personal information collected (more rigorous steps may be required when collecting 'sensitive information')
- the possible adverse consequences for an individual as a result of the collection

- any special needs of the individual (for example, whether the individual may have visual impairment)
- the practicability, including the time and costs involved. However, an entity is not excused from taking particular steps by reason only that it would be inconvenient, time-consuming or impose some cost.

In some situations an entity may decide that not taking any steps is reasonable in the circumstances. For example, this may be the case when an individual already knows the APP 5 matters because the personal information is collected from them regularly by the entity.

More information about what might be reasonable circumstances, and when it may be appropriate to take no steps, is provided in Chapter 5 of the APP Guidelines.

When and how should notice be given?

An individual may be notified or informed of APP 5 matters through a variety of formats. The way the personal information is collected, or later used, may suggest a particular form for the privacy notice. This includes whether the information is being collected directly from the individual or from a third party. Whether the personal information may be collected over the phone, by completing online forms, attending shopfronts, or through cookies also impacts how the notice may be given.

Privacy notices have a big job to do. They need to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful. The very technology that leads to greater collection of personal information also presents the opportunity for more dynamic, multi-layered and user centric privacy notices.

Innovative approaches to privacy notices can be adopted, for example 'just-in-time' notices, video notices and privacy dashboards.[9] Where possible privacy notices should be multi-layered and user centric to assist with readability and navigability. This means that brief notices are provided which are supplemented by longer notices. The timing of notices can also occur more dynamically to ensure information is given in context, at the right time, in a way that is easy to read.

Entities should use a PIA to consider how best to give notice of collection and the purpose of collection, especially for secondary uses such as big data activities. A PIA can consider the information lifecycle and help identify what information will be needed for which functions and activities of the entity. It can also identify how the personal information will be collected.

Risk point: Seeking consent at a later time for a secondary use of personal information for big data activities can be costly and difficult.

[9] 'Just-in-time notices work by appearing on the individual's screen at the point where they input personal data, providing a brief message explaining how the information they are about to provide will be used.' United Kingdom, Information Commissioner's Office, 'Just-in-time-notices', https://ico.org.uk/about-the-ico/privacy-notices-transparency-and-control/use-a-layered-approach/just-in-time-notices/.

Privacy tip: Entities should use a privacy impact assessment to consider how personal information will be used for big data activities. The PIA can be used to inform how and when a privacy notice that is meaningful to individuals should be given.

Dealing with personal information

The way entities deal with personal information depends on the purpose it was collected for and the privacy notice that was given to individuals. The privacy notice sets out how an entity can use and disclosure the personal information (APP 5 & 6). This includes for direct marketing purposes (APP 7), as well as the basis on which personal information may be sent overseas (APP 8).

APP 6 – Use and disclosure of personal information

APP 6 outlines when an entity may use or disclose personal information. It provides that personal information may only be used or disclosed for the purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies.

Using personal information for big data activities will generally be a secondary use of personal information. A secondary purpose is any purpose other than the primary purpose for which the entity collected the personal information.

The most common exceptions for the secondary use of personal information for big data include, where:

- the individual has consented
- the individual would reasonably expect the entity to use or disclosure their personal information for the secondary purpose (and that purpose is related to the primary purpose of collection)
- a permitted health situation exists.

The other exceptions are discussed in Chapter 6 of the APP guidelines.

The exceptions entities are likely to rely on for big data activities mean the privacy notices provided under APP 5 will be important. Entities may seek to rely on the consent of an individual to use the personal information for big data activities, and the privacy notice could be a key document in establishing express or implied consent.

Alternatively, a privacy notice may set out a range of likely secondary uses of personal information, including big data activities, which may help an entity establish that an individual would reasonably expect the use or disclosure. In relying on a privacy notice, entities should consider how they might allow individuals to choose which uses and disclosures they agree to and which they do not.

The individual has consented

An entity may use or disclose personal information for a secondary purpose where the individual has consented to that use or disclosure. Consent is defined as 'express consent or implied consent' (s 6(1)). The four key elements of consent are discussed in Chapter B (Key concepts) of the APP guidelines.

The individual would reasonably expect the use or disclosure

An entity may use or disclose personal information for a secondary purpose if the individual would reasonably expect the entity to use or disclose the information for that secondary purpose, and:

- if the information is sensitive information, the secondary purpose is directly related to the primary purpose of collection, or
- if the information is not sensitive information, the secondary purpose is related to the primary purpose of collection.

This exception creates a two-limb test which focuses both on the reasonable expectations of the individual, and the relationship between the primary and secondary purposes.

The 'reasonably expects' test is an objective one that has regard to what a reasonable person, who is properly informed, would expect in the circumstances. This is a question of fact in each individual case. It is the responsibility of the entity to be able to justify its conduct. The relationship between the primary and secondary purpose must be more than a tenuous link.

More information about 'reasonably expects' and the relationship between the primary and secondary purpose is provided in Chapter 6 of the APP Guidelines.

Permitted health situation

An entity may wish to use personal information for the secondary purpose of research. For organisations, the relevant APP 6 exception is where a permitted health situation exists. An organisation may use or disclose health information that is necessary for the secondary purpose of research relevant to public health or public safety if:

- it is impracticable to get the individual's consent
- the use or disclosure is conducted in accordance with the s 95A guidelines approved by the Information Commissioner
- for disclosure, the organisation reasonably believes the recipient will not disclose the information, or personal information derived from the information.[10]

Whether it is impracticable to seek consent will depend on the particular circumstances of the case. An organisation relying on this permitted health situation will need to justify

[10] See section 16B(3) of the *Privacy Act 1988*.

why it is impracticable to obtain an individual's consent. Incurring some expense or doing extra work to obtain consent would not itself make it impracticable to obtain consent.

An organisation seeking to rely on the section 95A guidelines must be satisfied that the research for which health information is to be used or disclosed has been approved by a Human Research Ethics Committee (HREC) in accordance with the guidelines. They may approve a proposed research activity where they determine that the public interest in the research activity substantially outweighs the public interest in the protection of privacy.

Agencies seeking to handle personal information for medical research in a way that may be inconsistent with the APPs should refer to section 95 of the Privacy Act.

Section 95 permits acts that would otherwise breach the APPs where those acts are done in the course of medical research and in accordance with guidelines issued under section 95 and approved by the Information Commissioner (s 95 guidelines).

The s 95 guidelines provide a framework for the conduct of medical research using information held or collected by agencies. An agency seeking to rely on the s 95 guidelines must be satisfied that the research for which the personal information is to be handled has been approved by an HREC for the particular purpose in accordance with the guidelines. In making a decision under these guidelines, a HREC must consider whether it is reasonable for the research to proceed without the consent of the individuals to whom the information relates. In addition, the proposed handling of information must be done in the course of medical research.

Risk point: Where health or personal information is being handled for big data activities it may be impracticable to obtain individuals' consent.

Privacy tip: Entities undertaking health or medical research should ensure they are familiar with the s 95 or s 95A guidelines.

More information about use and disclosure is provided in Chapter 6 of the APP Guidelines.

APP 7 – Direct marketing

Direct marketing is where an organisation directly promotes goods or services to an individual, and can encompass any communication made by or on behalf of an organisation to an individual.

APP 7 sets out when and how organisations can use and disclose personal information they hold for direct marketing purposes. Organisations can use and disclose personal information for direct marketing if:

- the organisation collected the personal information directly from the individual and the individual would reasonably expect their personal information to be used or disclosed for direct marketing
- the individual has consented to their personal information being used or disclosed for direct marketing

- it is impractical to get the individual's consent to their personal information being used or disclosed for direct marketing.

However, individuals' sensitive information can only be used and disclosed for direct marketing if the individual has given their consent.

In practice, many organisations undertaking big data activities will be doing so to inform their direct marketing activities. Specific requirements for direct marketing are set out under APP 7. This includes providing individuals with a simple means of opting out of future direct marketing communications and stopping their direct marketing where an individual asks them to stop.

Depending on the type of direct marketing communications organisations use to direct market to individuals, they may have other obligations that apply to their direct marketing communications, including the *Spam Act 2003* or the *Do Not Call Register Act 2006*.

For big data, it is also important to note that organisations that facilitate other organisations' direct marketing (such as data list brokers) also have specific obligations under APP 7. This includes no longer using or disclosing individuals' personal information where an individual has asked them to stop.

More information about APP 7, including the specific requirements, is provided in Chapter 7 of the APP guidelines.

Risk point: Organisations that *facilitate* other organisations' direct marketing have additional obligations under APP 7.

Privacy tip: Organisations should have a good understanding about how they use big data for direct marketing, and if this includes facilitating other organisations' direct marketing, they need to comply with additional obligations.

Using and disclosing personal information for direct marketing

One of the key purposes of big data analytics is to assist organisations to improve their marketing strategies. Where organisations use or disclose individuals' personal information to tailor the direct marketing communications (such as online advertisements) they send to and target at those individuals, they should consider the requirements of APP 7.

Due to the high volume of data organisations may collect for big data to inform direct marketing, and the range of information sources they may use, they should:

- ensure they keep track of the types of information they are collecting. This will reduce the risk of using or disclosing sensitive information for direct marketing purposes without individuals' consent
- consider individuals' expectations about how their information will be used and disclosed in light of the original purposes for which their information was collected and any notices they were provided

- think about how to implement simple and effective ways in which individuals can opt out of receiving direct marketing communications, or ask that their information is no longer used and disclosed for direct marketing purposes.

Organisations should also consider that even where APP 7 may not prevent them from using or disclosing customers' personal information for particular direct marketing purposes, building a good relationship with their customers is based on transparency and trust.

Risk point: The 2013 Community Attitudes to Privacy survey found that the majority of Australians are annoyed when they receive unsolicited marketing.

Privacy tip: Organisations should be transparent with their customers to build trust and avoid being 'creepy'.[11]

Using and disclosing personal information to facilitate direct marketing

There are a number of organisations that collect and analyse personal information on behalf of other organisations, or on-sell that information to organisations for use in their direct marketing activities.

It may be difficult in the big data context for such facilitating organisations to keep track of each individual's personal information. However, these organisations should be aware that individuals can ask that they stop using or disclosing their personal information to facilitate others direct marketing under APP 7 and consider implementing systems that will enable them to more easily meet this obligation.

APP 8 – Sending personal information overseas

APP 8 and s 16C of the Privacy Act apply when an entity discloses personal information overseas.[12] An organisation is considered to 'disclose' personal information where it provides the information to an overseas recipient, but does not maintain control over how that information is subsequently handled by the recipient.

APP 8.1 provides that, subject to certain exceptions set out in APP 8.2,[13] before an entity discloses personal information about an individual to an overseas recipient, the entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information.

[11] See 'Best Practice Guideline: Big Data', Association for Data-driven Marketing & Advertising, www.adma.com.au/assets/Uploads/Downloads/Big-Data-Best-Practice-Guidelines2.pdf.

[12] APP 8 does not apply where the entity maintains effective control over the information so that it would be considered to be 'using' rather than 'disclosing' the information. Instead, an entity 'using' personal information overseas will be accountable for its information handling under the APPs that apply to 'use'. In practice, the steps that an APP entity is required to take and their accountability when sending personal information overseas can be similar regardless of whether the information is being used or disclosed.

[13] See Chapter 8 of the APP guidelines, www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information.

These provisions are intended to enable individuals to seek redress in Australia, if their information is mishandled overseas.

Big data activities often involve using overseas cloud (or internet) based platforms. The APPs do not prevent the sending of personal information overseas or engaging an overseas cloud service provider. However, entities will need to carefully consider steps that may need to be taken to ensure compliance with the APPs.

Before an entity uses an overseas cloud service to store its data, or employs an overseas based cloud platform to perform big data analytics, it should consider whether it can achieve its aims using de-identified information. De-identification is discussed above.

Where it is necessary to disclose personal information overseas, an entity is required to take reasonable steps to ensure that the overseas recipient does not breach the APPs. Information about how to comply with APP 8 when sending information overseas is provided in our Privacy business resource 8: Sending personal information overseas and Privacy agency resource 4: Sending personal information overseas.

Where entities are likely to disclose personal information to overseas recipients they should include information about that disclosure in their APP 5 privacy notices. The APP 5 requirements are discussed above.

Risk point: Where an entity discloses personal information to an overseas recipient (unless an exception to APP 8 applies) it will be accountable for an act or practice of the overseas recipient that would breach the APPs. This is the case even if the entity has taken reasonable steps under APP 8.1.[14]

Privacy tip: Entities should undertake due diligence before disclosing personal information to overseas recipients. This will help them identify risks and take steps to mitigate them.

Maintaining personal information

This section of the guide provides guidance about how entities should maintain the personal information they are holding for big data activities. It addresses how entities should ensure the personal information it holds is accurate, up-to-date and complete. The reasonable steps entities should take to keep the vast amounts of personal information they hold for big data activities secure is also discussed.

APP 10 – Quality of personal information

Entities must take reasonable steps to ensure that the personal information they collect is accurate, up-to-date and complete (APP 10.1). Similarly, entities must take reasonable steps to ensure that the personal information it uses or discloses is - having regard to the purpose of the use or disclosure - accurate, up-to-date, complete and relevant.

[14] Section 16C of the Privacy Act.

Guidance about the meaning of the terms 'accurate', 'up-to-date', 'complete' and 'relevant' is provided in Chapter 10 of the APP Guidelines.

Taking reasonable steps

An entity must take reasonable steps to ensure the quality of personal information when it is collected, used or disclosed. This includes when personal information is collected via creation through big data activities (collection by creation is discussed above). The reasonable steps that an entity should take will depend upon circumstances and are discussed in Chapter 5 of the APP guidelines.

Big data and the quality of personal information

The nature of big data analytics means there is a higher risk that the personal information used, or collected via creation through analytics, may not be accurate, complete or up-to-date. This is because big data analytics uses large amounts of information, often collected from a variety of third party sources which may have been retained for long periods of time. Big data activities can also occur quickly, especially when the activity is for a time critical situation.

In these circumstances, more rigorous steps are likely to be required to ensure the quality of personal information. This is because where the quality of personal information is not ensured incorrect assumptions may be drawn about individuals or groups of people. Where those assumptions are acted upon there may be a detrimental impact on those individuals.

However the circumstances that may exist for big data analytics also mean some of the more typical ways of ensuring quality (for example verifying it with the affected individual) will be impracticable. There are however other steps entities may take, including:

- checking that third parties, from which personal information is collected, have implemented appropriate practices, procedures and systems to ensure the quality of personal information
- implementing procedures to help entities assess the quality of personal information. For example, recording when personal information is collected, whether it is an opinion and whether it was collected via creation.

Further discussion about the typical steps entities take is provided in Chapter 10 of the APP Guidelines.

Additionally, guidance about how individuals may seek access to the personal information entities hold about them and how they can seek correction of that information in certain circumstances is provided in Chapters 12 and 13 of the APP Guidelines.

Risk point: Where an entity collects personal information by creation there may be a higher risk that the information may not be accurate, complete and up-to-date.

Privacy tip: Entities may need to take more rigorous steps to ensure the personal information collected via creation is accurate, complete and up-to-date.

APP 11 – Security of personal information

APP 11 requires entities to actively consider whether they are permitted to retain personal information. When entities retain personal information, they must take reasonable steps to protect it from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

Guidance on the terms 'misuse', 'interference', 'loss', 'unauthorised access', 'unauthorised modification' and 'unauthorised disclosure' is provided in Chapter 11 of the APP guidelines.

Retaining personal information

APP 11 requires entities to actively consider whether they are permitted to retain personal information. When an entity no longer needs personal information for any purpose for which it may be used or disclosed under the APPs (and if the information is not contained in a Commonwealth record or legally required to be retained by the entity) the entity should destroy or de-identify the information. An entity must take reasonable steps to destroy or de-identify the personal information. De-identification is discussed above.

Where personal information is retained, entities should be able to justify their retention of the personal information. More information about the retention of personal information is provided in Chapter 11 of the APP Guidelines.

Risk point: Entities can only keep personal information they need for permitted purposes under the APPs. The onus is on entities to justify their retention of personal information.

Privacy tip: Entities should use a privacy impact assessment to assess what personal information they need and for what purposes. Entities need to be able to justify why they have retained personal information and for what permitted purposes. Entities can also consider de-identifying personal information so they can keep the data for future uses.

Reasonable steps for big data

Entities that engage in big data activities often hold larger amounts of data and for longer periods of time. Entities need to consider what security risks exist and take reasonable steps to protect the personal information they hold. This includes internal and external risks.

For example, holding larger amounts of personal information for longer may increase the risk of unauthorised access by staff or contractors. While 'honey pots' containing vast amounts of valuable data may increase the risk that an entity's information systems may be hacked.

It is expected that entities handling large amounts of personal information for big data purposes will conduct an information security risk assessment (also known as a threat risk

assessment) as part of undertaking a PIA. This will enable the entities to identify and evaluate security risks, including threats and vulnerabilities, and the potential impacts of these risks to personal information.

Undertaking an information security risk assessment will assist the entity to identify reasonable steps to take to protect personal information. This may include:

- limiting internal access to personal information to those who require access to do their job (i.e. providing access on a 'need to know' basis)
- maintaining a chronological record of system activities, such as an audit log, by both internal and external users, for reviewing activity on a ICT system to detect and investigate privacy incidents
- implementing network security measures, such as intrusion prevention and detection systems, which can be an effective way of identifying and responding to known attack profiles
- undertaking penetration testing of enterprise data warehouses to identify internal and external vulnerabilities to mitigate against
- utilising encryption to ensure that information is stored in a form that cannot be easily understood by unauthorised individuals or entities
- implementing the Privacy Management framework
- ensuring reasonable steps are taken to destroy or de-identify the personal information when it is no longer needed
- in the event of a data breach, having a response plan that includes procedures and clear lines of authority which can assist an entity to contain the breach and manage their response.

More information about reasonable steps, including further examples of what may be reasonable steps, is provided in the *Guide to securing personal information*.

Risk point: 'Honey pots' of valuable and sensitive personal information may be targets for hacking.

Privacy tip: Undertaking an information security risk assessment will enable entities to identify reasonable steps to take to protect the personal information they hold.

Appendix A – additional resources

Guide to undertaking privacy impact assessments.

The *Guide to undertaking privacy impact assessments* provides assistance to entities on designing, conducting and acting on a privacy impact assessment.

Guide to developing an APP privacy policy

APP 1 requires entities to have a clearly expressed and up-to-date privacy policy describing how they manage personal information. An APP privacy policy is a key document to ensure personal information is managed in an open and transparent way.

Guide to securing personal information

The *Guide to securing personal information* provides guidance on the reasonable steps entities are required to take under the Privacy Act to protect the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure. It also includes information about the reasonable steps entitles are required to take to destroy or de-identify personal information they hold once it is no longer needed (unless an exception applies).

Privacy business resource 4: De-identification of data and information and Information Policy agency resource 1: De-identification of data and information

This resource provides guidance on when de-identification may be appropriate, how to choose appropriate de-identification techniques and how to assess the risk of re-identification.

The Australian Public Service Big Data Strategy

The OAIC participated in the development of the Australian Public Service Big Data Strategy which was launched in August 2013. Privacy is a crucial plank of the strategy, with good privacy practice recognised as enabling big data activities while maintaining citizen trust.