Australian Privacy Law Handbook

SAMPLE PAGES

PRESIDIAN
LEGAL PUBLICATIONS

[17]

Privacy Act 1988

[19]

Coverage

[This space is intentionally blank]

Information to which Act applies

[19.235] The Privacy Act only applies to "personal information," as defined by the Act (the information must also be kept within a record – see [19.255]). Accordingly, not all information held by an organisation is subject to the Act.

Within personal information, there are two sub-categories; namely, sensitive information and health information. In certain instances, the APPs relate specifically to these sub-categories of information.

Personal information

Related materials
- OVPC, *Guidelines to the IPPs* (3rd ed, 2011) at pp 7-14 (under "Personal information")

[19.240] As a broad rule of thumb, "personal information" is information about an individual. The specific definition under the Privacy Act is as follows (s 6(1)):

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

The fact that personal information includes opinions, whether true or not, means it encompasses, for example, medical opinions (including a misdiagnosis, even though it is incorrect) and opinions about customers noted in records by sales staff.

Personal information extends to information about an individual contained in images (see [19.260]), such as photographs (see, eg, *Smith v Victoria Police* [2005] VCAT 654).

The types of information that may constitute personal information are limitless. Types of personal information commonly held by entities include address, contact details and transaction history. Other types of information that have been held to constitute personal information include:

- information about a bankrupt's estate in bankruptcy (*Pullen v Joiner a Trustee of The Property of Kevin Michael Pullen a Bankrupt* [2013] FMCA 172);
- fingerprints (*Complainant AB v Victoria Police* [2006] VPrivCmr 3);
- surveillance footage (*Ng v Department of Education and Training* [2005] VCAT 1054) and reports (*Complainant X v CSP to a Department* [2005] VPrivCmr 6; *Complainant AE v CSP to a Statutory Authority* [2006] VPrivCmr 6); and
- a university student's PhD candidature (*Complainant F v Tertiary Institution* [2003] VPrivCmr 6).

The Privacy Commissioner has found that a person's name is, in itself, personal information and does not have to be linked with other information to fall within the meaning of the term: *Own motion investigation report, Telstra Corporation Limited (Telstra)* (OAIC, 2011). However, in *Pullen*, Jarrett FM came to a different conclusion. His Honour stated (at [13]-[14]):

> In a different context it has been held that disclosure of the name of a person is not necessarily the disclosure of information concerning the personal affairs of that person. Whether it does so will be a question of fact to be determined depending upon the circumstances of each particular case. [*Commissioner of Police v District Court of NSW* (1993) 31 NSWLR 606]
>
> The terms of s.6 of the Act draw a distinction between the notion that the relevant information or opinion is *about* a person and that person's identity. That is to say, the mere identification of a person in or by information or an opinion is insufficient to engage the definition of *personal information*. The definition clearly requires more than mere identification – the information or opinion must be *about* that person. (original emphasis)

The Commissioner interprets the meaning of personal information to exclude information about a deceased person (as "individual" is defined as meaning a natural person (s 6(1))) (*APPG* at [B.89]). In contrast, health records statutes are expressly stated to apply to information about deceased individuals (usually for a specified period following death).

Biometric information (such as fingerprints and iris scans) and body samples (such as hair and blood) will generally constitute personal information when held by an entity that has the means to analyse and identify an individual or link the information with identifying information (eg an employer or a forensic laboratory vs a member of the public): OVPC, *Guidelines to the IPPs* (3rd ed, 2011) at p 12.

Since the word "individual" is defined as meaning a natural person and the definition of personal information requires an individual's identity to be apparent or reasonably ascertainable from it, where the only identity apparent or reasonably ascertainable from the information is that of a corporation or some other form of association, the information will fall outside the definition of personal information. However, information that is primarily about a corporation or some other form of association but which also reveals information about an individual whose identity is apparent (for example, information about who is a corporation's managing director), then that information is personal information in relation to the individual. See the case summary of *J v Utility Company and IG* [2006] PrivCmrA 9 below.

Whether information is solicited or unsolicited has no bearing on whether the information falls within the meaning "personal information": see, eg, *E v Private School* [2010] PrivCmrA 6.

"Personal information" includes two sub-categories of information; namely, "sensitive information" and "health information". These two sub-categories of personal information are, in certain instances, regulated separately from personal information generally under the Act. The meaning of these terms is considered at [19.245] and [19.250] respectively.

"About" a reasonably identifiable individual

[19.240A] The definition of personal information requires, among other things, that information be "about an ... individual". In *Telstra Corporation Limited and Privacy Commissioner* [2015] AATA 991, Deputy President Forgie of the Administrative Appeals Tribunal adopted a narrow interpretation of when information is "about an individual" which significantly limits the scope of the definition in comparison with the broader interpretation previously adopted by the Privacy Commissioner. The Commissioner has appealed the decision to the Federal Court of Australia.

In *Telstra*, a customer ("complainant") of the appellant telecommunications company, Telstra, lodged a request for access to a range of personal information it held about him. Telstra provided access to various categories of personal information (eg date, time and duration of calls) but refused access to mobile network data (eg IP addresses, signalling data, cell tower location) ("metadata"). At first instance (*Grubb and Telstra Corporation Limited* [2015] AICmr 35), the Commissioner determined that the metadata was "about an individual" because Telstra could cross match it with other identifying information on its network and records management systems (something Telstra did regularly in response to requests from law enforcement agencies to assist in identifying individuals) (at [52]-[53]). This was consistent with previous findings and guidelines issued by the Commissioner (see [19.241]). On appeal, Deputy President Forgie found that the metadata was not information "about an individual" on the basis that it was "information about the service it provides to [the complainant] but not about him". Examples given by Deputy President Forgie in the decision (see further below) indicate that the decision, if upheld, will have significant implications for all entities as it applies not only to metadata but also to any records (eg hardcopy reports) that, in Deputy President Forgie's analysis, can be categorised as being about the service provided by the entity, rather than the individual to whom the service relates.

The decision in *Telstra* was concerned with the definition of personal information prior to its amendment as part of the Privacy Act reforms in March 2014. However, the definition does not appear to have been amended in any relevant way. The pre-amendment definition referred to "information ... about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion" and the post-amendment definition refers to "information ... about an identified individual, or an individual who is reasonably identifiable" (emphases added). Accordingly, the relevant element of the definition, being that the information must be "about an individual", remains the same.

Deputy President Forgie held, based on the definition of "personal information", that the assessment of whether information is "about an individual" is the first step in the process of characterising whether information is personal information. Further, this must be determined irrespective of whether the information can be linked with other identifying information. If not, the information is not personal information. Deputy President Forgie stated (at [95]):

> [W]hen applying the definition of "personal information" under ... the Privacy Act, the questions that are asked must be framed in terms of the definition. They cannot be asked against a different frame of reference that has, as its starting point, the question: is it possible to use this information or opinion or to marry it with other information by using a computerised search engine or in some other way to ascertain the identity of an individual. The starting point must be whether the information or opinion is about an individual. If it is not, that is an end of the matter and it does not matter whether that information or opinion could be married with other information to identify a particular individual.

At first instance, the Commissioner had indicated that the test for whether information is "about an individual" is whether it is "in some way concerning or connected with the individual": *Grubb*, above, at [48]. Likewise, Deputy President Forgie held information is "about" an individual if it is "concerning or relating to [them]; on the subject of them" (at [97]).

Deputy President Forgie held that whether information is about an individual requires an analysis of the subject matter of the information and that, whilst the information may concern or relate to an individual, an assessment must be made of whether the connection with the individual is too tenuous (at [98]-[99]). If so, it will not be personal information. To demonstrate, Deputy President Forgie

gave an example of a road accident in which a car runs a red light and hits a pedestrian. If an accident report names the driver and the pedestrian and describes the circumstances of the accident, the report as a whole could be said to be about the driver, the pedestrian and the circumstances of the accident. However, whilst the driver's identity may be able to be traced back to information in the report and in medical records relating to the pedestrian's treatment, the link with the driver would be too tenuous for those records to be characterised as being "about" the driver and, as such, would not be personal information about him or her (at [99]-[100]).

Similarly, Deputy President Forgie gave an example (at [96]) relating to the repair of a car part pursuant to a warranty. Service records noting problems related to the part, the order for its replacement and its replacement would be information about the part or the car and the repairs. However, they would not be information about the car owner, even if the records included his or her name. Likewise, if the service records did not contain the owner's name, even if they could be matched with sales records for the car to ascertain the identity of the owner, this would not change the nature of the information in them, being information about the car, the part or the repairs but not about the owner.

In relation to the matter before her, Deputy President Forgie stated (at [111]-[112]):

> I also accept that it may, but not always, be possible to identify a particular Telstra customer by reference to the mobile network data and other data it maintains. That fact does not necessarily lead to the conclusion that the mobile network data is personal information. Whether it is personal information depends upon its characterisation as being about an individual for that is what the definition of "personal information" requires. [The complainant] submitted that, but for his making his calls or sending his SMS or MMS messages, particular data in Telstra's mobile network data would not have been generated. That is true but it does not detract from the characterisation task that I am required to undertake. Is the information about an individual being, in this case, [the complainant] or is it about something else? If the outcome of that characterisation is that it is not information about an individual, Telstra will not, as [the complainant] submitted, be required to keep it secure under the Privacy Act. That is an outcome that would follow from the application of the definition in the particular circumstances of the case.
>
> ... [Telstra] generated that data in order to transmit [the complainant's] calls and his messages. Once his call or message was transmitted from the first cell that received it from his mobile device, the data that was generated was directed to delivering the call or message to its intended recipient. That data is no longer about [the complainant] or the fact that he made a call or sent a message or about the number or address to which he sent it. It is not about the content of the call or the message. The data is all about the way in which Telstra delivers the call or the message. That is not about [the complainant]. It could be said that the mobile network data relates to the way in which Telstra delivers the service or product for which [the complainant] pays. That does not make the data information about [the complainant]. It is information about the service it provides to [the complainant] but not about him. (emphasis added)

Deputy President Forgie noted that Telstra kept billing information and mobile network data "separate and distinct" (at [46]). If the decision is upheld, this suggests that storing information about a service (as opposed to information about a customer) in databases separate from those containing identified customer information may assist in justifying classifying that data as "non-personal information". For example, an electricity distributor that maintains a database containing non-identified information about electricity usage at specific sites, but which also holds identified billing information relating to premises in a separate database, may be able to justify classifying the electricity usage database as non-personal information even though information in the two databases can be matched via property addresses.

Ironically, for carriage service providers and content service providers, such as Telstra, the commencement of s 187LA ("Application of the *Privacy Act 1988*") of the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act) on 13 October 2015 (several months after the Commissioner's determination) as part of the Government's data retention scheme means that mobile network data is generally classified as personal information for the purposes of the Privacy Act, effectively negating any impact of the decision in *Telstra* for such service providers. Section 187LA provides that activities of such providers that relate to data retained pursuant to s 187A of the TIA

Act are bound by, and the information is deemed to be personal information for the purposes of, the Privacy Act.

Whilst the decision in *Telstra* has implications beyond solely metadata, understanding what constitutes "metadata" is important. In the context of the Government's data retention scheme under the TIA Act, the scope of the term (used interchangeably with "communications data" and "telecommunications data") was discussed in various documents during the proposal phase. The Attorney-General's Department's *Discussion Paper, Equipping Australia against emerging and evolving threats* (2012) notes in the context of communications data (at p 25):

> The concept of 'data' is not defined in the TIA Act but is generally understood to refer to information about a communication that is not the content or substance of a communication. Data is increasingly understood as falling into two categories: subscriber data, which provides information about a party to a communication such as name or billing address; and traffic data, which relates to how a communication passes across a network, such as the location from which the communication was made.

In *Telstra*, Deputy President Forgie found that mobile network data has two essential features: firstly, that it records transactions occurring between mobile devices and the mobile network in order to manage the mobility of mobile devices through that network; and, secondly, that it establishes, maintains or disconnects connections between mobile devices and the destinations (eg another mobile device, a fixed service or an internet location).

In relation to IP addresses, Deputy President Forgie held (at [113]) that the IP address allocated to a mobile phone is not personal information, on the basis that it is not allocated exclusively to a particular mobile device and a particular device is not allocated a single IP address over the course of its life. As such, an IP address for a mobile device is ephemeral and is not about the person but about the means by which data is transmitted to and from the device. However, this arguably is not applicable to fixed IP addresses for computers as these generally do not change.

"Reasonably identifiable" individual

[19.241] Information about an individual will be personal information if the individual is "identified" or "reasonably identifiable" (see [19.240]).

The fact that information does not directly state or reveal an individual's name (ie it appears on its surface to be de-identified) does not in itself mean that it is not personal information (see *X v Transport Company* [2007] PrivCmrA 26 below under "Cases") as it may still be possible to ascertain someone's identity from the information; for example:

- due to its singular nature or uniqueness (*La Trobe University*, above) – for example, where it is clear from the context in which information is given, such as where a young person living in unusual circumstances sees a counsellor in relation to a particular problem and then calls the counsellor anonymously the following week seeking help with a different problem but describing those same unusual circumstances.

  In *Q and Financial Institution* [2011] AICmrCN 11, C contracted with a buyer to sell his car which was under finance with the respondent finance company (FC) which had a security interest in the car. FC sent the buyer a letter stating the amount outstanding on the car had been paid and that it would discharge its security interest. The letter only contained details about C's vehicle and did not mention C's name or account number. The Commissioner held that the prospective buyer was able to reasonably ascertain that the details in the letter related to C's account with FC and the information contained in the letter was therefore personal information within the meaning of the Act;
- by matching the information with other information that identifies an individual – for example, by linking a customer number, or a database containing purely statistical data about customer transaction histories or utility services usage data, with a customer database containing customer account details that identifies the customers. In *Baptist Union of Queensland – Carinity v Roberts* [2015] FCA 1068, Rangiah J observed (at [52]) that one of the purposes of the amendment to the definition of "personal information" in the 2014 reforms

"was to expand the scope of the protected information to information which can be linked with other information to identify an individual";

- where it contains unique identifiers, such as birth dates, which enable data subjects to be identified by third parties who know their birth dates.

Whether a person's identity can be *reasonably* ascertained must be assessed "taking into account the likelihood, cost, difficulty and practicality of that occurring": *Baptist Union of Queensland – Carinity v Roberts* [2015] FCA 1068 at [53] per Rangiah J.

Whether an identity can reasonably be identified will depend on the circumstances. Relevant considerations will include (*APPG* at [B.85]):

- the nature and amount of information;
- the circumstances of its receipt;
- who will have access to the information;
- other information either held by or available to the entity;
- whether it is possible to identify the individual using available resources (if so, the practicability, including the time and cost involved, will be relevant);
- if the information is publicly released, whether a reasonable member of the public who accesses that information would be able to identify the individual.

For example (*APPG* at [B.86]):

- for most entities, a licence plate number is not personal information as they do not have access to car registration databases providing plate holder names (however, in the hands of an entity that does have access to such a database, it would be personal information);
- information that an unnamed person with a certain medical condition lives in a specific postcode area may not for most entities be personal information as they cannot link the information with an individual (however, if the same information was in the hands of an entity with specific knowledge of who that record related to, it would be personal information).

Another key consideration will be the resources available to the entity (eg financial and other information assets) which may facilitate matching the relevant data with identifying information. The test is whether it is "beyond what is reasonable relative to the resources it has at its disposal and its existing operational capacities": *Grubb*, above, at [100] (overruled in *Telstra*, above (pending appeal)). In *Grubb* (for the facts of the case, see [19.240A]), the Commissioner held that, whilst extracting the metadata required interrogation of several of Telstra's information systems by a group of specifically qualified personnel, which required a significant amount of time, the complainant's identity could reasonably be ascertained by Telstra from the metadata (at [93], [121]). In making this finding, the Commissioner took into account the fact that Telstra is a large organisation with "many resources at its disposal", including a pool of over 120 staff with expertise in data retrieval who were already specifically engaged in the retrieval and cross-matching of metadata in response to requests from law enforcement bodies or to problem-solve customer connectivity service or performance issues (at [94]).

Whether it is sufficient that only a single, or small group, of persons would be able to ascertain the individual's identity from the information is unclear. In *Baptist*, a case involving a third party application to inspect documents, Rangiah J observed (at [54]) that this is a potentially difficult issue but did not need to be resolved in that case.

In *X v Transport Company* [2007] PrivCmrA 26, the Privacy Commissioner stated:

> [f]or the identity of an individual to be reasonably ascertained from information there must be some likelihood that other individuals are in a position to identify the person who is the subject of the information. It is not sufficient that those individuals might identify the subject of the information.

In *WL v La Trobe University (General)* [2005] VCAT 2592, La Trobe University, the respondent, was collaborating with other research institutions in a study. The applicant's partner was a participant in part of that study. The partner had been contacted by a survey interviewer from Hunter Valley Research Foundation ("HVRF"), the organisation contracted to conduct the data collection for

[7]

Annotated Australian Privacy Principles

Introduction

Related materials
- Commentary on the Privacy Act reforms at [52]
- *APP Guidelines* (OAIC, 2014) (APPG)
- *APPs and NPPs – Comparison Guide: Summary and analysis of key differences for organisations* (April 2013)
- *APPs and IPPs – Comparison Guide: Summary and analysis of key differences for agencies* (2013)
- *Privacy business resource 2: Privacy Act reforms – Checklist for APP entities (organisations)* (2013)
- *Privacy agency resource 2: Privacy Act reforms – Checklist for APP entities (agencies)* (2013)

[7.10] The Australian Privacy Principles (APPs) commenced operation on 14 March 2014 and were introduced into the Privacy Act by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which implemented the major legislative elements of the federal Government's first stage of Privacy Act reforms (for commentary on the reforms, see [52.05]). The APPs replaced both the private sector NPPs and the public sector IPPs under the Privacy Act.

The APPs represent principles-based law, being high-level principles to guide entities' data management practices. It is the responsibility of each entity to determine how the APPs apply in the context of the specific circumstances and data management practices of the entity concerned. The APPs adopt a technology-neutral approach to ensure they are applicable to all current and future types of technologies.

Annotated Australian Privacy Principles

Part 1—Consideration of personal information privacy

[7.100] Australian Privacy Principle 1—open and transparent management of personal information

1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up-to-date policy (the ***APP privacy policy***) about the management of personal information by the entity.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

Overview of APP 1

[7.120] APP 1 requires APP entities to manage personal information in an open and transparent way and to adopt a *proactive* approach to privacy compliance (ie foreseeing privacy risks and putting systems in place to avoid such risks eventuating). The principle applies a "privacy by design" approach, requiring privacy and data protection compliance to be included in the design of information systems from their inception.

"Practices, procedures and systems" to ensure compliance (APP 1.2)

Related materials
- OAIC, *Privacy management framework* (2015)
- OVPC, *Privacy by Design: Effective Privacy Management in the Victorian public sector* (2014)
- Information and Privacy Commissioner of Ontario, *Privacy by Design* standard and materials at <www.privacybydesign.ca>
- Information and Privacy Commission NSW, *Privacy Governance Framework* (2014) (provides guidance for NSW agencies on elements of a robust privacy governance framework)

[7.140] To comply with APP 1.2 obligations to have in place "practices, procedures and systems" to ensure compliance with the APPs, entities should have in place comprehensive privacy compliance programs. Typically, this entails developing a privacy compliance plan (or privacy management plan) that sets out control measures the entity will adopt to minimise and manage privacy risks and to meet compliance obligations under applicable privacy principles. Control measures will generally comprise information management policies, procedures and systems.

A privacy compliance plan should encompass the following types of control measures (see also *APPG* at [1.7]):

- privacy collection notices
- privacy consents
- privacy policy
- collection forms
- internal information management policies
- information management procedure manuals and guidelines (aimed at identifying and managing privacy risks)
- information systems design
- data security policies and procedures
- data destruction policy and procedures
- document retention policy
- privacy clauses in contracts
- access and correction procedures
- complaint handling procedures
- staff training
- monitoring program
- review program
- consideration of conducting a privacy impact assessment where new, or significant changes in, information handling practices are proposed
- role of Privacy Officer
- incident reporting and response management.

The OAIC's *Privacy management framework* (2015) provides non-binding general guidance on steps the Commissioner expects entities to take to meet APP 1.2 obligations. The framework outlines four steps an entity should take to ensure good privacy governance, comprising:

- step 1 – embed a culture of privacy that enables compliance;
- step 2 – establish robust and effective privacy processes;
- step 3 – evaluate privacy processes to ensure continued effectiveness;
- step 4 – enhance responses to privacy issues.

The requirement to have in place practices, procedures and systems to ensure compliance with the APPs encourages entities to adopt a privacy by design approach when developing new systems and processes involving the handling of personal information. *Privacy by Design*, developed by the Information and Privacy Commissioner of Ontario in the 1990s (available at <www.privacybydesign.ca>), is a globally recognised standard for enabling privacy to be built-in to the design and architecture of information systems, business processes and networked infrastructure. It aims to ensure that privacy is considered before, at the start of, and throughout the development and implementation of initiatives that involve the collection and handling of personal information. The standard, comprising 7 Foundational Principles, was recognised as the global standard in a resolution by the International Conference of Data Protection and Privacy Commissioners in Jerusalem in October 2010. The standard was formally adopted by the Victorian Privacy Commissioner in July 2014 as a core policy to underpin information privacy management in the Victorian public sector. The Victorian Commissioner has also published *Privacy by Design: Effective Privacy Management in the Victorian public sector* (2014), a background paper designed to assist Victorian Government organisations to adopt a privacy by design approach, based on the global standard, to personal information. These resources provide useful guidance for all public and private sector entities aiming to ensure privacy is built-in to new systems and processes.

Comparison with former NPPs and IPPs

[7.160] Neither the NPPs nor IPPs contained an express requirement to implement practices, procedures and systems to ensure compliance with the principles. However, for entities that had in place such measures as part of their privacy compliance programs, APP 1.2(a) had little impact as it is merely formalised practical measures already implemented. However, for entities that had *not* developed compliance programs under the NPPs and IPPs, APP 1.2(a) had a significant impact as it expressly required them to do so.

"Reasonable steps" test (APP 1.2)

The reasonable steps that an APP entity should take will depend upon the circumstances. Relevant considerations include (see further *APPG* at [1.6]):

- the amount and sensitivity of information held;
- the severity of consequences if information is not handled in accordance with the APPs;
- the nature of the entity – relevant considerations include size, resources and business model (eg centralised entity, franchise, dealership network or highly outsourced structure);
- practicability (eg amount of time and costs involved and whether these are excessive).

Dealing with enquiries and complaints about compliance (APP 1(2)(b))

[7.180] The obligation under APP 1.2(b) to have in place practices, procedures and systems to enable an entity "to deal with inquiries or complaints" about compliance with the APPs requires entities to have privacy enquiry and complaint handling mechanisms. These can form part of an entity's broader mechanisms for handling enquiries and complaints of all types.

"Such steps as are reasonable in the circumstances" (APP 1.2)

[7.220] Commentary on the meaning of the phrase "such steps as are reasonable in the circumstances" is set out at [7.25].

Privacy policy (APPs 1.3-1.6)

Related materials
- OAIC, *Guide to developing an APP privacy policy* (2014)
- Commentary on developing privacy policies at [117.10]

[7.240] APP 1.3 requires an entity to have a clearly expressed and up-to-date privacy policy about its management of personal information. The policy is not expected to contain detail about all the practices, procedures and systems adopted to ensure APP compliance (*APPG* at [1.10]).

An "up-to-date" privacy policy means the policy should be a living document that is reviewed regularly to ensure it accurately reflects current practices. The Commissioner has indicated a "review could, at a minimum, be undertaken as part of an entity's annual planning processes" and "could include a notation on the policy indicating when it was last updated" (*APPG* at [1.9]).

The legislative note to APP 1.5 confirms that having a privacy policy available on the entity's website is sufficient. For agencies, online privacy policies should also comply with the *Web Content Accessibility Guidelines 2.0*, which are mandatory for federal, State and Territory government websites and contain a number of requirements for making web content more accessible for people with disabilities: OAIC, *ACT Justice and Community Safety portfolio: Assessment report* (2015) at [3.6]. If an entity does not have an online presence, see *APPG* at [1.40] for ways in which a privacy policy may be made available.

An entity may have multiple, or separate, privacy policies. For example, in addition to a central privacy policy, an entity may have separate privacy policies that relate to, for example, a particular business unit, product or service. The federal Commissioner supports the use of such policies as they provide more detailed and meaningful information about data management practices (in contrast, the Commissioner has indicated that an online privacy policy should not relate solely to information collected through the relevant website – a common flaw in many policies – as this is not sufficient to meet the content requirements stipulated in APP 1.4 (see OAIC, *ACT Justice and Community Safety portfolio: Assessment report* (2015) (JACS Report) at [3.32]) – this distinction appears to be on the basis that it is helpful and meaningful for policies to be specific to business unit/product/service, but not to medium/technology used to handle information): JACS Report at [3.35]. Multiple policies are often appropriate, for example, for large entities that have information handling practices that are diverse, or which are significantly different within different business units or for different products or services, and a single policy could not meaningfully cover all relevant practices without being too lengthy or cumbersome. Accordingly, in addition to a central Customer Privacy Policy, an entity may, for example, also have a Service Provider Privacy Policy, a Product X Privacy Policy, a Joint Venture Privacy Policy (for a business it is undertaking with another entity) or an HR Privacy Policy. An entity should, however, be careful to ensure that it is clear which policy applies to which activity. For example, an entity with different privacy policies for different online products should ensure that the webpage for each product, or the page where each is made available for download, contains a prominent link to the relevant policy and does not only contain a "standard" privacy link leading to a general privacy policy the entity maintains, as this could be misleading.

If it is foreseeable that the policy may be accessed by individuals with special needs (eg vision impaired or non-English speakers), appropriate accessibility measures should be put in place (*APPG* at [1.36]).

For commentary on drafting privacy policies, including in condensed/layered format, see [117.10].

Assessment reports

Objective of assessment was to assess online privacy policies of seven agencies within ACT Justice and Community Safety (JACS) Directorate portfolio against specific and key requirements of TPP 1 (equivalent to APP 1) – criteria against which policies assessed were accessibility (TPP 1.5), readability (TPP 1.3), contactability (TPP 1.4) and content (TPP 1.4) –

Part 2—Collection of personal information

[7.998] Australian Privacy Principle 3—collection of solicited personal information

Overview of APP 3

[7.1020] APP 3 prohibits the collection of personal information by an entity unless the information is "reasonably necessary" for one of the entity's functions or activities (or, for agencies, if it is "directly related" to a function or activity).

The collection of "sensitive information" (a subset of personal information, defined in s 6(1)) is regulated under APPs 3.3 and 3.4 which generally provide that sensitive information can only be collected where the collection:

- is with consent and meets the "necessity" test under APP 3.3; or
- falls within an exception under APP 3.4.

Information must be collected by lawful and fair means (APP 3.5) and directly from the individual concerned unless it is unreasonable or impracticable to do so (or, for agencies, if the individual consents or collection from a third party is required or authorised by law) (APP 3.6).

It is a relatively common misconception that public sector agencies cannot collect personal information from private sector organisations or, at least, that different requirements apply in these circumstances. However, there is no difference in obligations in regard to whether an entity from which information is being collected by an agency is in the public sector (eg another agency) or the private sector (eg an employment agency, a private sector law firm, a GP or an individual). The APPs apply in the same way to both types of collection.

Comparison with former NPPs and IPPs

[7.1040] APP 3 obligations reflect those that existed under NPP 1.1 and IPP 1.1 to only collect information that is "necessary" for a function or activity.

Notable new exceptions under APP 3.4 that permit collections of sensitive information without consent where it was not so permitted under NPP 10 included ones relating to:

- unlawful activity or serious misconduct – this enables, for example, an organisation to maintain a database of individuals who have engaged in criminal activities (eg theft) against it as a means of protecting its assets (this was effectively prevented under NPP 10 – see, eg, *I v Retail Company* [2006] PrivCmrA 8);
- alternative dispute resolution processes – this effectively extended the exemption under NPP 10.1(e) regarding legal claims to also cover processes such as mediation and conciliation.

Sensitive information was regulated separately under NPP 10 but not under the IPPs, which did not distinguish between the two types of information. Accordingly, the regulation of sensitive information as a subset of personal information was a new concept for agencies.

Under the reforms, the definition of "sensitive information" was expanded to include biometric information (see the last two dot-points below). The full meaning of "sensitive information" is (s 6(1)):

- information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs,

membership of a professional or trade association, membership of a trade union, sexual orientation or practices or criminal record;

- health information about an individual;
- genetic information about an individual that is not otherwise health information;
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

"Biometric templates" are generally digital representations of biometric features formulated using algorithms. Many biometric recognition systems compare these to identify individuals.

In regard to private sector organisations, the extension of the definition of sensitive information to include biometric information impacted those that use biometric technologies, such as access controls that incorporate fingerprint and iris scanners. The primary implication of the change was that consent is needed to collect biometric information. However, in many cases, such information is in any case collected with consent as it is primarily collected directly from the individuals concerned, which generally means consent to collection is implicit.

APPs 3.3 and 3.4 had a significant impact on agencies' collection practices. Many agencies collect large amounts of sensitive information; for example:

- information about racial origin and religious beliefs (eg when handling discrimination complaints);
- health information (eg about clients and employees);
- criminal records (eg when conducting background checks); and
- biometric information (eg for use in relation to biometric access controls).

Agencies needed to review what types of sensitive information they collected and ensure the collections complied with APP 3 requirements. Agencies needed to look closely at collections that occurred without consent to ensure they were permitted under one of the exceptions.

"Collect"

[7.1045] Collection includes the acquisition of personal information from any source, by any means and in any form (see former *NPPG* p 22). This is so irrespective of whether the information was sought by the organisation: *M v Financial Institution* [2009] PrivCmrA 16.

An entity "collects" personal information for the purposes of the Privacy Act "only if the entity collects the personal information for inclusion in a record or generally available publication" (s 6(1)). This concept applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means. In practice, all personal information that is held by an entity will generally be treated as information that was collected by the entity (*APPG* at [3.5]). For further guidance, see *APPG* at [B.17].

The fact that the Act applies to a collection of information that is to be included in a generally available publication is not inconsistent with the fact that such information will not be subject to the Act once it is included in such a publication (see [19.255]). It simply means that the information will be regulated by the Act during the period from when it is collected to when it is included in the generally available publication – see [19.255].

In *Seven Network v Media Entertainment and Arts Alliance* [2004] FCA 637, the respondent failed to lead acceptable evidence on how it obtained information in order to protect the identity of the source of the information. The court held (at [45]) that this led to an inference that any such evidence would not assist its case and that some active step was taken to obtain the information.

[7.1088]

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

"Reasonably necessary"

Related materials
- OVPC, *Guidelines to the IPPs* (3rd ed, 2011) at p 31 (under "Necessity")

[7.1090] APP 3.1 prohibits the collection of personal information unless it is "reasonably necessary" for a "function or activity". The Commissioner has stated (*APPG* at [3.8]):

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

The "reasonably necessary" test is an objective test: "whether a reasonable person who is properly informed would agree that the collection is necessary. Generally, personal information will be deemed "necessary" if an entity cannot effectively pursue a legitimate function or activity without collecting it (see *NPPG* p 27). Being necessary for the doing of something means something that "is reasonably required and ancillary to its achievement": *'HW' and Freelancer International Pty Limited* [2015] AICmr 86 at [226]. Information will not be deemed necessary if it is collected merely because it is helpful, desirable or convenient (*APPG* at [B.107]). The fact that information might be required in the future (as opposed to it being required for a planned future function or activity, but will not be used immediately) is not sufficient (*APPG* at [3.19], [3.21]). A collection of information will not usually be considered reasonably necessary if there are reasonable alternatives available, for example, if de-identified information would be sufficient for the relevant function or activity (*APPG* at B.109]).

The Privacy Commissioner provided guidance on the meaning of "necessary" in *Tenants' Union of Queensland Inc v TICA Default Tenancy Control Pty Ltd* [2004] PrivCmrACD 4 (*Complaint Determination No. 4 of 2004*). The Commissioner stated (at [48]-[49]):

> … I note…the comments of Gummow J in *General Newspapers Pty Limited and Others v Telstra Corporation* (1993) 117 ALR 629 (considering the meaning of 'necessary' within section 236(1) of the *Telecommunications Act 1991*):
>
> > The term 'necessary' will take its colour from its context; in ordinary usage it may mean, at one end of the scale, 'indispensable' and at the other end 'useful' or 'expedient': *Re an Inquiry under the Company Securities (Insider Dealing) Act 1985* [1988] AC 660 at 704.
>
> I find that the use of the word 'necessary'… falls between the two ends of the scale identified by Gummow J. In my view it does not require that the information be indispensable to an organisation, in that, without such information, it would be impossible to carry on its business. It will not, however, be sufficient to show that the information is merely 'useful' or 'expedient'. Rather, determining whether or not the collection of personal information is 'necessary' requires consideration of whether or not it is clearly appropriate and relevant to the functions or activities of the organisation. In my view, information that is only of marginal relevance to the functions or activities of an organisation is more likely to be considered unnecessary for the purposes of NPP 1.1. It will also be relevant to consider whether or not the functions or activities of the

> organisation can be reasonably performed in a manner which does not require the collection of personal information. It may also be relevant to consider whether the information is of a sensitive nature such that it may be considered to be more invasive of a person's privacy. (emphasis added)

The interpretation in *Tenants' Union of Queensland* gives "support to the notion that collection has to be relevant rather than crucial to the organisation's functions and activities": *'HW' and Freelancer International Pty Limited* [2015] AICmr 86 at [34].

It is the responsibility of an APP entity to be able to justify that the particular collection is reasonably necessary" (*APPG* at [3.18]). Relevant considerations in determining this include (*APPG* at [3.19]):

- the primary purpose of collection;
- how the information will be used in undertaking the relevant function or activity;
- whether the entity could undertake the function or activity without collecting the information, or by collecting a lesser amount of information.

APPs 3.1 and 3.2 mean that an entity cannot collect information for which it has no current or planned future need. One way in which entities often breach this principle is by requesting irrelevant information from customers on application forms, either because the question directly requests irrelevant information or, more commonly, because the question is drafted too broadly.

However, where personal information is collected in the context of providing a particular good or service, APPs 3.1 and 3.2 do not mean that the entity cannot request information for other purposes at the same time. For example, a credit union loan application form may request information that will be used by the credit union for marketing purposes. Whilst the marketing information will not be needed for loan assessment purposes, the information is "necessary" for marketing activities it conducts and its collection will therefore generally be permitted under APP 3.2.

Where an organisation collects separate pieces of personal information that are both necessary and unnecessary respectively, it should consider taking steps to avoid collecting the unnecessary pieces. For example, an organisation taking a photocopy of a driver's licence could block out the drivers licence number and organ donor information if these bits of information on the licence are not required. Similarly, when collecting date of birth (DOB) details for ID verification, it may be appropriate to collect truncated DOBs comprising solely of month and year (ie do not include day) where this is sufficient, in conjunction with name and address, to identify the individual concerned. This may, in particular, be appropriate where DOBs will be published, for example, on a website registry.

Cases

Collection forms

[7.1091] An online form provided by an agency for job applicants asked applicants to advise whether they had ever suffered from a work-related injury or illness. The collection of information was not required by any law nor was it relevant to the process of recruitment and selection. *Outcome:* The Commissioner didn't make a formal finding, but indicated the collection was not necessary (and, as such, was likely to have been a breach). The agency amended its recruitment practices accordingly and verified that no applicant had been disadvantaged by the collection: *Own Motion Investigation v Australian Government Agency* [2007] PrivCmrA 4.

C, a bus driver, was required to submit a completed Medical Assessment Form to renew his public passenger vehicle driver's licence. The form asked: "Have you ever had any serious injury, illness, operation or been in hospital for any reason? Yes No If yes, give details". *Outcome*: The information required in response to the question was not reasonably necessary for the purpose of determining whether an applicant met the relevant medical fitness criteria and breached HPP 1 of the *Health Records and Information Privacy Act 2002* (NSW). The question "cas[t] a very wide net" and was designed to capture information in relation to any serious injury, illness, operation which an applicant has ever had, irrespective of its relevance to medical fitness to drive a public

passenger vehicle. The question sought details of every time an applicant had been in hospital, irrespective of the relevance of that information to fitness to drive: *JK v Department of Transport Infrastructure Development* [2009] NSWADT 307.

A bank required marital status information from C who wished to open a bank account. C objected on the grounds that it was unnecessary for the purposes of opening the account, but the bank advised that its system did not allow certain accounts to be opened without entering information in the 'marital status' field. The bank stated that modifications to its system to enable individuals to open accounts without disclosing marital status would take some time and proposed that, to open an account for C, it would enter "single" in the data field and include a note stating that the entry may not reflect actual marital status. The bank agreed that the collection of marital status information was not necessary as it had no bearing on C's eligibility to open the account. *Outcome*: The bank agreed that it would change its computer system so that an individual could refuse to provide marital status information. The banking institution committed to providing the Commissioner with quarterly reports on the progress of its implementation program. The bank also resolved to raise the issue of marital status collection with its industry body as it appeared to be an industry-wide practice: *D v Banking Institution* [2006] PrivCmrA 4.

The respondent, an employment services company, had been requiring applicants to provide a large amount of personal information, including tax file numbers and credit card details. *Outcome*: Requiring applicants to provide credit card details on application forms was an unnecessary collection of information and breached NPP 1.1 as an individual who had obtained a placement did not have to pay by credit card. The respondent removed the requests on forms for credit card details: *OPC v Employment Services Company* [2005] PrivCmrA 13.

Consent forms

An insurer's privacy consent forms were drafted broadly to enable it to obtain any information from C's health service providers, without limiting the consent to information that was relevant to a claim. The consent form provided "I authorise any medical attendant consulted by me or any hospital attended by me, to divulge to [the insurer] or any legal tribunal, any health or other information acquired with regard to myself." Further, the form did not limit the period for which the consent was valid. The statement was found to breach NPP 1.1 on the grounds that its application was not limited to personal information which would be relevant to the claim in question. The insurer amended its forms so that only information relevant to a claim could be collected and by limiting the authority's validity to the period during which a claim was being assessed. The investigation was closed on the grounds that the insurer had adequately dealt with the matter: *N v Private Insurer* [2003] PrivCmrA 12.

Surveillance

The applicant, an employee with a Commonwealth Government department, had had his employment terminated for using a work laptop at home outside of business hours using his own internet service provider (ISP) to view pornography in breach of the workplace Information and Communications Technology (ICT) Policy and, in turn, the Australian Public Service Code of Conduct which required compliance with that policy. The Department discovered the access as a result of software it had installed on the laptop which monitored internet activity, including websites visited. The software logged keyword searches and took desktop screenshots every 30 seconds which were relayed to a dedicated server. The applicant sought orders quashing the decisions that he had breached the Australian Public Service Code of Conduct and that the appropriate sanction was termination of his employment. The applicant argued the Department had breached IPP 1(1) on the basis that the information collected relating to his personal use of the laptop outside of work using his own ISP was not necessary for any purpose of the Department. *Outcome:* The Department did not breach IPP 1(1) as the collection of information

Part 3—Dealing with personal information

[7.2500] Australian Privacy Principle 6—use or disclosure of personal information

Related materials
- OAIC, *Business resource: Using and disclosing patients' health information* (2015) (DRAFT)
- CPDP, *Guidelines for sharing of personal information* (2016)
- ICOUK, *Data sharing checklists*
- ICOUK, *Data sharing between different local authority departments*
- ICOUK, *Data sharing code of practice*
- ICOUK, *The use and disclosure of information about business people*
- PCNZ, *A Guide For Journalists* (regarding disclosures by agencies to journalists)

Overview of APP 6

[7.2503] APP 6 sets out the circumstances in and purposes for which an entity may use or disclose personal information.

APP 6.1 authorises an entity to use and disclose personal information solely for the primary purpose for which it was collected (in relation to the meaning of primary purpose of collection, see [7.2528]). APP 6.2 and 6.3 set out a series of exceptions that permit use or disclosure for a secondary purpose. A secondary purpose is any purpose other than the primary purpose for which the entity collected the personal information (*APPG* at [6.14]).

For agencies, many primarily make disclosures to other agencies. However, it is often necessary for agencies to make disclosures to private sector entities; for example, to:

- contracted service providers;
- workers' unions;
- health service providers;
- employment agencies; and
- legal advisers.

The requirements regarding the purposes for which a disclosure may be made are generally the same, regardless of whether the entity to which the information is being disclosed is in the private or public sector. As such, provided the disclosure is permitted under APP 6, it is generally irrelevant whether the receiving entity is in the private or public sector.

The table below sets out the secondary uses and disclosures permitted under APP 6, along with those that were permitted under the former NPPs and IPPs.

"Disclosure" deemed as "use" where control over data retained

Related materials
- OAIC, *Privacy business resource 8: Sending personal information overseas* (2015)
- OAIC, *Privacy agency resource 4: Sending personal information overseas* (2015)

[7.2508] In most cases, the provision of personal information to a third party will constitute a disclosure (*APPG* at [B.61]). However, in limited circumstances, provision of information to a third party may be deemed a use rather than a disclosure. The Commissioner has stated (*APPG* at [B.138]):

> This occurs where the entity does not release the subsequent handling of personal information from its effective control. For example, if an entity provides personal information to a cloud service provider for the limited purpose of performing the services of storing and ensuring the entity may access the personal information, this may be a 'use' by the entity in the following circumstances:
>
> a) a binding contract between the entity and the provider requires the provider only to handle the personal information for these limited purposes
> b) the contract requires any subcontractors to agree to the same obligations, and
> c) the contract gives the entity effective control of how the information is handled by the provider. Issues to consider include whether the entity retains the right or power to access, change or retrieve the information, who else will be able to access the information and for what purposes, the security measures that will be used for the storage and management of the personal information ... and whether the information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.

However, provision of information to a third party in the following circumstances is generally considered a disclosure (*APPG* at [8.13]):

- the provision of information about customers by a retailer outsourcing the processing of online purchases to a contractor;
- the provision of information about job applicants by an entity to a contractor engaged to conduct reference checks;
- the provision of access to a customer database to a parent company that provides technical and billing support.

Where the provision of information to a third party is deemed to be a use rather than a disclosure, an APP entity may breach the APPs if the information is mishandled while in the third party's possession on the basis that it is considered to still "hold" the information and various APPs (eg APP 6 regarding permitted uses and disclosures) apply to an entity that "holds" personal information: *APPG* at Ch 8 (v1.1) at [8.15]. Conversely, APPs which only apply in relation to disclosures (eg APPs 1.4(f), (g) and 5.2(f), (i), (j) regarding notification in privacy collection notices and privacy policies of entities to which disclosures are made, overseas disclosures and recipient countries)

generally do not apply to such deemed uses (therefore, in the examples given, notification of such "uses" arguably does not need to be given in collection notices and privacy policies - see *APPG* at [1.29], [5.29]).

Cases

C lodged an application with the Administrative Appeals Tribunal (AAT) regarding a decision made by an agency. During the AAT application process, the agency obtained C's fingerprints and provided these to a law enforcement body for the purpose of verifying the authenticity of documents considered relevant to the AAT application. C complained that the agency had improperly collected their personal information. The law enforcement body was aware that the information was provided for the sole purpose of fingerprint analysis on the documents submitted by the agency and, in line with its standard procedure, destroyed the information when advised to do so by the agency which the agency would do once the AAT review was concluded. *Outcome:* The transfer to the law enforcement body was a use, and not a disclosure, of personal information by the agency for the purpose of checking the veracity of the documents (permitted under IPP 10): *J and Commonwealth Agency* [2011] AICmrCN 4.

C had lodged several complaints against an agency relating to their conditions of employment with the agency. The agency engaged a contractor to investigate its handling of the complaints and gave the contractor a copy of C's personnel and related files to be used solely for the purposes of the investigation. The contractor was also required to return its copy of C's information to the agency at the conclusion of its investigation, which it did. C complained that the agency improperly disclosed their personal information to the contractor without consent. *Outcome:* The disclosure to and use by the *contractor* was a deemed use by the *agency*. The agency had maintained control over C's information as the information was given for the sole purpose of investigating C's allegations and the contractor returned its copy of the information at the conclusion of its investigation: *N v Commonwealth Agency* [2009] PrivCmrA 17.

Uses/disclosures prohibited by another law

[7.2509] There are numerous laws which prohibit the use and disclosure of information that would otherwise be permitted under the APPs. Examples of such laws include:

- an agency's governing statute might prohibit certain uses and disclosures;
- secrecy provisions not to disclose information;
- common law duties of confidence – these generally prohibit the disclosure, and sometimes the use for secondary purposes, of confidential information.

The APPs do not *compel* uses or disclosures in any circumstances. Rather, they *authorise* them for specified purposes. Accordingly, if a particular use or disclosure is prohibited under another law, the entity must comply with that other law.

Where a use or disclosure is required or authorised by another law, APP 6.2(b) generally permits such a use or disclosure even if it is otherwise not permitted under the APPs – see [7.2625].

Compulsorily acquired information (agencies only)

[7.2510] A government agency that obtains information in the exercise of a statutory power to obtain information for a particular purpose is subject to a duty of confidentiality in relation to that information, even if the information is not otherwise confidential, such that the agency may not use or disclose it except for the purpose for which it was obtained. In *Johns v Australian Securities Commission* (1993) 178 CLR 408; [1993] HCA 56, Brennan J stated:

> the purpose for which a power to require disclosure of information is conferred limits the purpose for which the information disclosed can lawfully be disseminated or used …

A statute which confers a power to obtain information for a purpose defines, expressly or impliedly, the purpose for which the information when obtained can be used or disclosed. The statute imposes on the person who obtains information in exercise of the power a duty not to disclose the information obtained except for that purpose. If it were otherwise, the definition of the particular purpose would impose no limit on the use or disclosure of the information. The person obtaining information in exercise of such a statutory power must therefore treat the information obtained as confidential whether or not the information is otherwise of a confidential nature.

Scope of exemptions

[7.2511] Exceptions permitting secondary uses and disclosures generally only apply to the extent necessary. For example, if an exception authorises secondary disclosure of medical records about a patient to a treating specialist, the exception will only authorise disclosure of medical records that are relevant to the ailment being treated by the specialist. It will not authorise disclosure of all of the patient's medical records.

Cases

The applicant teacher lodged a worker's compensation claim against the school at which he taught. The school principal disclosed to a consulting psychologist involved in assessing the claim information the school had received via an anonymous phone call relating to the applicant's behaviour and alleged problems at another school at which he had taught. The applicant claimed the school and the responsible government Department had disclosed and used the information contrary to s 18 (disclosure) of the *Privacy and Personal Information Protection Act 1998* (NSW). *Held:* The Department breached s 18 as the disclosure of that particular information was not necessary for the purpose of enabling psychologist to determine the merit of the applicant's work cover claim: *VK v Department of Education & Training (No 3)* [2011] NSWADT 168.

Public interest determinations authorising disclosures

[7.2516] The OAIC has issued the public interest determinations listed below authorising disclosures that would otherwise breach the APPs.

Determination	Description	Commencement	Expiry
Privacy (International Money Transfers) Generalising Determination 2015	To permit authorised deposit-taking institutions to disclose the personal information of a beneficiary of an international money transfer (IMT) to an overseas financial institution when processing an IMT (a generalising determination)	25.2.2015	25.2.2020
Privacy (International Money Transfers) Public Interest Determination 2015 (No. 1)	To permit ANZ Banking Group to disclose personal information of a beneficiary of an international money transfer (IMT) to an overseas financial institution when processing an IMT	25.2.2015	25.2.2020
Privacy (International Money Transfers) Public Interest Determination 2015 (No. 2)	To permit the Reserve Bank of Australia to disclose the personal information of a beneficiary of an international money transfer (IMT) to an overseas financial institution when processing an IMT	25.2.2015	25.2.2020
Public Interest Determination No. 5	To permit the Australian Federal Police to disclose personal information relating to homicides in the ACT to the Australian Institute of Criminology	4.12.1991	1.10.2018

Public Interest Determination No. 3A	To permit disclosure of personal information to relevant statutory disciplinary or regulatory bodies	14.12.1991	1.10.2018
Public Interest Determination No. 2	To allow certain disclosures for the purpose of considering applications for the Australian honours system	12.11.1990	1.10.2018

Cases

Contents

Disclosures to family member/former spouse or partner

[7.2523.3] The respondent club received a court subpoena relating to family law proceedings involving C and their ex-partner. The subpoena directed the club to provide to the court all gambling records, or records of transactions linked to any gambling cards related to or held in the name of C or C's company. The letter directed the club to give the documents to the ex-partner by 28 November 2005. In September 2007, being almost two years later, the club provided to the ex-partner computer printouts of C's full membership details and C's player activity statements for periods in 2002 and 2003. The statements showed C's total turnover and winnings and account balance. *Outcome:* The disclosure breached NPP 2.1. The disclosure was not authorised by law under NPP 2.1(g) as it was

not made in accordance with the requirements of the subpoena, having been made several years after the date required by the subpoena. Based on medical evidence, the Commissioner found that the disclosure caused C non-economic loss, including injury to C's feelings and humiliation, and partly caused serious anxiety, panic attacks and physical symptoms (other unrelated causes included disputes with C's ex-partner over a property settlement, child support and child custody). Given the combined pressures on the complainant it is a difficult task to determine to what extent the anxiety, panic attacks and physical symptoms were caused by the Club's disclosure. However, I am of the view that the disclosure caused injury to the complainant's feelings and humiliation even if a proportion of their anxiety and physical symptoms had other causes. The Commissioner made a s 52 determination requiring the club to: apologise in writing to C; review and undertake within six months staff training regarding handling personal information and legal requests for such information including court subpoenas; and pay C compensation of $7,500 for non-economic loss: *'D' and Wentworthville Leagues Club* [2011] AICmr 9.

C purchased items from a home shopping retailer (R) as an unexpected gift for their spouse (S). S later telephoned R to purchase items and an employee disclosed to S that C had purchased items, revealing the nature of the gift. C and S approached R about the disclosure, seeking financial compensation for the stress and anxiety they suffered as a result of the disclosure and an undertaking that R would not discuss the matter with other employees, nor disclose their personal information to another party. C was dissatisfied with R's response. *Outcome:* R resolved the matter by reminding staff about the impact of handling customers' personal information, undertaking to monitor calls for quality and privacy matters, confirming that no record of the disclosure or the complaint was kept (preventing further discussion of the incident) and by issuing C a written apology and a substantial discount on the item that was to be a gift: *J v Home Shopping Retailer* [2008] PrivCmrA 10.

Disclosure by a financial institution's staff member of information about an account holder to the staff member's family was held not to be covered by any of the exemptions under NPP 2.1. Further, while the institution could show when the information had been modified, an inability to show when it had been accessed by a staff member was held to result in an increased risk of breaching NPP 2.1. The Commissioner indicated that the organisation should take appropriate IT measures to ensure that access to financial information is monitored in the future: *E v Financial Institution* [2003] PrivCmrA 3.

C and their ex-spouse used a community centre for the handover of care of their children. C alleged that the centre had disclosed to their ex-spouse copies of letters C had sent to the centre. *Outcome*: There was no breach. The centre implemented a range of data security measures including a "clean desk" policy, storing client information in locked cabinets and drawers, and ensuring that personal information that was no longer required by the centre was securely disposed of. There was no evidence to show that C's personal information had been disclosed to the ex-spouse: *T v Private Community Centre* [2008] PrivCmrA 20.

C was a member of a licensed club. Two individuals, one of whom was C's ex-partner, told the club manager that they were friends of C and the manager disclosed C's home address to them. C received phone calls which resulted in C feeling unsafe and relocating. C sought compensation for relocation costs and subsequent loss of income. A club representative failed to attend a meeting arranged with C to address the complaint. *Outcome*: The club agreed to pay C an undisclosed amount of compensation in settlement of the complaint: *A v Licensed Club* [2007] PrivCmrA 1.

C paid a retailer (R) a deposit for a fridge which was to be delivered once the balance was paid. However, the fridge was delivered to C's house before the balance was paid. C did not pay the balance and refused to return the fridge. Several months later the husband (H) of the sales person (SP) who took the deposit attended C's residence on two occasions requesting that C return the fridge or pay the outstanding money. Later, SP and H attended C's residence. SP claimed that she was being threatened with dismissal over the incident. C alleged that R had interfered with their privacy

[7.2525]

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the ***primary purpose***), the entity must not use or disclose the information for another purpose (the ***secondary purpose***) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

"Primary purpose of collection"

Related materials

- OPC, *Information Sheet 23 – Use and disclosure of health information for management, funding and monitoring of a health service* (2008)
- OPC, *Information Sheet 25 – Sharing health information to provide a health service* (2008)

[7.2528] The primary purpose of collection is the particular purpose for which information was collected by the entity, even if the entity intends to use the information for additional purposes (*APPG* at [B.92]-[B.93]). For example, if a bank collects an individual's personal information on a loan application form, the primary purpose of collection will generally be to provide financial services. Similarly, if a retailer collects personal information from a customer returning a faulty product for repair under a warranty, the primary purpose of collection would be to service the warranty. If an entity uses or discloses information for any purpose other than the primary purpose of collection, this is for a secondary purpose (*APPG* at [6.14]).

The primary purpose may be described in general terms, as long as the description is adequate to inform an individual of the purpose of collection. It could, for example, be "to provide banking services", "assess an applicant's suitability for a job" or "to resolve a complaint". However, a description such as "for the functions of the entity" would be unacceptably broad (*APPG* at [B.96]).

If an entity provides more than one product or service in a single transaction, the primary purpose attaches to each product or service such that, instead of there being more than one primary purpose, there is a single primary purpose to provide each product or service (*GPPHS* p 12).

Where personal information is collected from a person other than the individual concerned, the primary purpose of collection will generally be the purpose for which it is used in relation to the individual, eg where a business receives a tender application from a potential supplier and obtains information about the applicant from an industry member, the primary purpose of collection is to assess the applicant's tender (see ExpMem1 note 320; *GPPHS* p 12).

Where a health service provider treats a patient in a single appointment for more than one unrelated injury or illness, the primary purpose attaches to each service such that there will be a single primary purpose to treat the patient for each injury or illness (see *GPPHS* p 12). This construction of the

meaning of the "primary purpose of collection" is arguably not wide enough to encompass, in addition to the episode of health care during which the information is collected, all future episodes of health care for the patient. If so, this is not consistent with a holistic approach to health care that many health service providers adopt whereby health information is used in the treatment of future injuries and illnesses from which the patient may suffer. In view of this, health service providers should consider obtaining consent at the time of collection to use and disclose health information for future episodes of health care.

In *Seven Network v Media Entertainment and Arts Alliance* [2004] FCA 637, the court considered whether a disclosure by a principal to an agent was for the primary purpose of collection. The respondent had engaged a call centre to poll employees regarding an enterprise agreement. The applicant argued that information disclosed by the call centre to the respondent was for an unrelated secondary purpose. *Gyles J* held (at [53]): "I am not satisfied that there is a primary and a secondary purpose in an agency situation like the present. If there is, then the better view is that the primary purpose is that of the principal … In any event, if there are two purposes, they were directly related".

It has been held under Victorian privacy legislation that, where a person lodges a complaint with an organisation about an individual, it is arguably part of the primary purpose of collection to show the complaint to the individual concerned in the interests of natural justice: *Complainant AG v Local Council* [2007] VPrivCmr 2.

Cases

Telstra Corporation's privacy statement stated it used personal information to: assist customers to subscribe to its services; administer and manage those services; research, develop and improve services; gain an understanding of customer information to provide better services; and maintain and develop Telstra's business systems and infrastructure. C's personal information was used for publication in the White Pages, as required by the terms of Telstra's carrier licence. *Outcome:* The primary purpose of collection was to deliver services to which customers had subscribed. The discharge of Telstra's obligations under its carrier licence did not fall within this purpose. Publication of the information was for the secondary purpose of Telstra meeting the conditions of its carrier licence: *'DK' and Telstra Corporation Limited* [2014] AICmr 118.

C lodged an application with the Administrative Appeals Tribunal (AAT) regarding a decision made by an agency. During the AAT application process, the agency obtained C's fingerprints and used these to verify the authenticity of documents considered relevant to the AAT application (the fingerprints were disclosed to a law enforcement agency for analysis, but this was a deemed use rather than a disclosure). C complained that the agency had improperly handled their personal information. *Outcome:* The use of the fingerprints was consistent with their purpose of collection, being to check the veracity of the documents, and was authorised under IPP 10: *J and Commonwealth Agency* [2011] AICmrCN 4.

C told a private school (S) they were considering legal action against S. S replied that it would defend any legal action. In an attempt to conciliate the matter, C sent S a copy of their intended legal claim. The Commissioner found that the primary purpose for which S collected the information was to defend, or avoid, any legal action brought by C: *E v Private School* [2010] PrivCmrA 6.

The personnel division of an agency sent C's CV to another division of the agency for it to assess C's eligibility for a vacancy within the area. The CV was five years old. C alleged that use of the old CV to assess their suitability for the position was not a use for the purpose for which it was collected. *Outcome:* The agency did not breach IPP 10. The use of the CV to assess qualifications and experience relevant to the position was a use for which the information was originally collected: *M v Commonwealth Agency* [2003] PrivCmrA 11.

[This space is intentionally blank]

[7.2575]

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

"Reasonably expect"

Related materials
- OVPC, *Guidelines to the IPPs* (3rd ed, 2011) at pp 52-55 (under "Reasonably expected")

[7.2578] 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 (*APPG* at [6.20]). The Commissioner has provided the following guidance on how to apply the test (*APPG* at [6.21]):

> An APP entity should consider whether an individual would reasonably expect it to use or disclose for a secondary purpose only some of the personal information it holds about the individual, rather than all of the personal information it holds. The entity should only use or disclose the minimum amount of personal information sufficient for the secondary purpose. For example, an individual may not reasonably expect an entity that is investigating their complaint against a contractor to disclose the individual's residential address and home contact details to the contractor as part of its investigation. The individual would reasonably expect the entity to give the contractor only the minimum amount of personal information necessary to enable them to respond to the complaint.

In determining whether a use or disclosure is within the individual's reasonable expectations, relevant considerations will include (*NPPG* p 36):

- whether the individual knew, or whether it was clear from the circumstances surrounding the collection, that the information may be used for the secondary purpose (evidence that the entity provided the individual with a privacy collection notice indicating that the information may be used for the secondary purpose will strong evidence of this);
- the level of confidentiality or sensitivity that attaches to the information (if it is high, reasonable expectations as to secondary purposes will be more restricted);

- whether it is accepted industry practice to use or disclose the information for the secondary purpose (eg many businesses disclose information to mailing houses for mailing purposes); and
- whether the entity is under a duty of care or bound by a professional code of conduct or professional standards of which the individual would reasonably be aware and which would require the organisation to make the secondary use or disclosure (eg a lawyer's professional duty to ensure that accurate advice is given regarding a client's personal liability may require the lawyer to use the individual's information to make relevant enquiries about the individual).

In determining what an individual would reasonably expect, an individual should be taken to have no special knowledge of the relevant industry or activity (*NPPG* p 36).

To maximise the possibility that a secondary purpose is within an individual's reasonable expectations, an entity should ensure that the individual is notified of the primary purpose of collection through the provision of a privacy collection notice so that his or her reasonable expectations are determined in view of that information. If possible, the entity should also state in the notice the secondary purposes for which the information will be used and disclosed. In this instance, it would be difficult for the individual to argue that use or disclosure for such purposes was not within their reasonable expectations.

Examples of uses and disclosures for secondary purposes within reasonable expectations may include (*APPG* at [6.22]):

- where an individual makes adverse comments in the media about how an entity has treated them – responding publicly in a way that reveals personal information specifically relevant to the issues raised by the individual;
- disclosing information after notifying the individual about the disclosure in an APP 5.1 privacy collection notice;
- uses and disclosures for normal internal business practice (eg auditing and billing).

It is important to note that, while a use or disclosure may generally be within most peoples' reasonable expectations, it may not be within a particular individual's reasonable expectations, particularly where he or she has indicated that he or she would like information to be handled in a specific manner that is not in accordance with normal information handling practices. It is best practice to accord with such wishes, even if a particular use or disclosure may otherwise be authorised under NPP 2.1(a).

In the context of health services, an individual's reasonable expectations are likely to be influenced by factors that may not be relevant in other contexts due to the sensitive nature of health information. When assessing an individual's reasonable expectations, a health service provider should have regard to factors such as the individual's (*GPPHS* p 13):

- age and level of maturity;
- general understanding of how the health system operates (a basic understanding will indicate that he or she realises, for example, that general practitioners often make disclosures to specialists – the level of understanding may be affected by factors such as the individual's economic or social background); and
- cultural views of specific health issues (eg an Islamic woman of a Middle-Eastern background may consider certain female health issues to be much more sensitive than a young Australian woman).

It is accepted industry practice, and necessary, for health service providers to share information about patients with specialists and other members of treating teams. In view of this, it will often be within an individual's reasonable expectations for two or more of his or her health service providers to share information about him or her where necessary. However, providers should nevertheless notify individuals about such practices through privacy collection notices and privacy policies.

Cases

Directories. Telstra Corporation collected C's personal information for the primary purpose of providing a phone line. Telstra subsequently used C's information for the secondary purpose of publication in the White Pages, as required by the terms of its carrier licence. C was not informed such use would occur and no privacy statements contained information to this effect. *Outcome:* Such secondary use was not within C's reasonable expectations: *'DK' and Telstra Corporation Limited* [2014] AICmr 118.

C had a combined listed phone and fax number, but C paid a fee to have the address suppressed in directories. C acquired a dedicated fax number which was subsequently listed by the telephone company (TC) in the directories. Due to a processing error, an address was included. *Outcome*: When upgrading, C could not have reasonably expected that their address would be disclosed and, as such, TC failed the reasonable expectations test and breached NPP 2.1(a). The parties came to a confidential settlement: *W v Telecommunications Company* [2007] PrivCmrA 25.

Sample forms. A health insurer included sensitive information in a sample form and disclosed the form to employers as an example of the form that their employees would be sent if they fell into arrears with their payments. *Outcome*: The disclosure was not within reasonable expectations: *B v Private Health Insurer* [2002] PrivCmrA 2.

"Reasonably aware" (under former IPP 11.1(a)). C, an employee of the respondent Department, lodged a worker's compensation claim. C signed a consent to the disclosure of his records to relevant parties (including any health professional) in the course of managing his claim. The Department sent C a letter requesting him to undertake a medical assessment with an independent medical practitioner and notifying him that the resulting report may be disclosed his treating doctor and medical specialists. The independent practitioner recommended that C not be provided with a copy of the report, but that it be provided to him through his treating doctor. By email, the respondent requested C to notify them if he did not give consent to this. C refused consent. The Department subsequently provided a copy of the report to C's treating GP. C claimed the disclosure: exacerbated his anxiety and depression; increased his loss of confidence, panic and fear, particularly in the context of returning to work; caused lack of sleep, poor concentration and an inability to regard his future positively; lengthened his rehabilitation period and increased family tensions. *Outcome:* The disclosure breached the IPPs. C was not aware of the independent practitioner's recommendation. It was not reasonably likely C would have been aware the report would be disclosed to his GP. Pursuant to a s 52 declaration, the Department was required to: make a written apology; amend its information handling procedures and submit them to the OAIC for review; train staff in the new procedures; pay $5,000 compensation for non-economic loss: *'CP' and Department of Defence* [2014] AICmr 88 at [28].

The applicant had applied for a visa. As part of this process, the applicant's wife from whom the applicant had separated, had written a letter containing personal information to the Department processing the visa application. The applicant sought access to the letter, but the Department refused the request on the basis that it contained personal information about a third party who would not be reasonably likely to have been aware that the information would be disclosed to the applicant. *Outcome*: The wife was not likely to have been aware that the letter was of a type that was usually passed to the visa applicant and access could be denied: *Maman v Minister for Immigration* [2011] FMCA 426.

C, a Commonwealth agency employee, applied for work at another agency and named their supervisor as a referee. The relevant position was primarily as a call centre operator. The supervisor disclosed to the interview panel that C suffered from epilepsy and depression, was on sick leave and did not cope well under stress. C's application was unsuccessful. C claimed this was due to the disclosures by the referee and lodged a complaint about the disclosures. *Outcome:*

The disclosure of information about epilepsy and sick leave breached IPP 11.1(a). C was not reasonably likely to be aware that the referee would disclose medical information in the course of providing a reference. The disclosure regarding C's ability to cope with stress did not breach IPP 11 as this information was relevant to employment, particularly for a position as a call centre operator. C was reasonably likely to be aware that judgements of this kind could be conveyed by the referee. The agency apologised to C and paid compensation of $7,000: *C v Commonwealth Agency* [2003] PrivCmrA 1.

C sent two emails to an agency alleging a third party, an agency affiliate that received agency funding, had misused funds. The agency's privacy policy stated that email messages provided to it would not be disclosed without the sender's consent. Despite this, an officer of the agency forwarded the two emails to the third party. The third party instituted defamation proceedings against C on the basis of the emails. The parties reached a settlement out of court. *Outcome:* The agency was not entitled to rely on IPP 11.1(a) to justify the disclosure to the third party. In view of the agency's privacy policy (which required consent for disclosure), C could not have been reasonably likely to have been aware that the emails would have been forwarded to the third party. The fact that C had sent one of the emails to other entities in addition to the agency did not negate the agency's responsibility to comply with its privacy policy: *N v Australian Government Agency* [2005] PrivCmrA 12.

C was an employee of an agency. The agency had undertaken an investigation into C's conduct. C later submitted a workers' compensation claim and the agency arranged for a doctor to assess C to determine their fitness for duties. The agency notified C that the purpose of the doctor's appointment was to assess their ability to return to the workplace and that it would provide the doctor with personal information about C. The information subsequently provided by the agency to the doctor included information relating to the investigation. The subject matter of the investigation was relevant to the assessment of C's condition. C claimed the agency had no need to disclose this information. *Outcome:* The disclosure was permitted under IPP 11.1(a). C was reasonably likely to have been aware (even if not actually aware) that the information would be passed to the doctor because of the prior notifications they had received. It is usual practice in workers compensation matters for an employer to provide an assessing doctor with all relevant information about the employee. As the subject matter of the agency's investigation may have presented a barrier to C returning to work, the information was relevant to the assessment of C's condition: *J v Commonwealth Agency* [2009] PrivCmrA 13.

"Related" and "directly related"

[7.2580] A "related secondary purpose is one which is connected to or associated with the primary purpose. There must be more than a tenuous link" (*APPG* at [6.24]). A "directly related secondary purpose is one which is closely associated with the primary purpose, even if it is not strictly necessary to achieve that primary purpose" (*APPG* at [6.26]).

Examples of a secondary purpose that is related to the primary purpose of collection and within reasonable expectations include (*APPG* at [6.25]):

- a law firm, acting as debt collector for an organisation, collects information for the primary purpose of collecting an individual's debt. The firm asks the individual's neighbour about the individual's whereabouts without disclosing any details about the debt;
- an agency uses information contained in an employee's personnel file, which was originally collected for the primary purpose of administering the individual's employment, as part of an investigation into a workplace complaint;
- de-identifying personal information.

Examples of uses and disclosures that will be directly related secondary purposes will generally include using or disclosing information for (see generally *DNPPG* p 70):

- administrative purposes (eg account keeping, billing);
- management and funding purposes (eg preparation of budgets, provision of client specific discounts);
- quality review purposes (eg assessment of provision of services, product reviews, procedural audits);
- entering into legal arrangements (eg disclosing information to a lawyer or an insurer in relation to organising professional indemnity insurance);
- customer relations purposes (eg notification that a product is ready for collection or that offices will be closed for business on a given date);
- referral purposes (eg to refer a customer to an alternative temporary supplier until stocks are replenished);
- customer awareness purposes (eg a solicitor notifying a client of a new law that will significantly affect the client's activities);
- service renewal or expiry notification (eg an insurer notifying a policy holder that his or her policy will soon expire); and
- the out-sourcing of services that are commonly contracted out (eg customer enquiries, mailing, the provision of cheques and credit cards, electronic network administration and printing).

Cases

C had lodged several complaints against an agency relating to their conditions of employment with the agency. The agency engaged a contractor to investigate the complaints and, for the purposes of the investigation, gave the contractor a copy of C's personnel and related files. The agency maintained control over C's information and, consequently, the "disclosure" to and subsequent use by the contractor was deemed to be a "use" by the agency by the Commissioner. *Outcome:* The agency's use of C's personal information for the purpose of the investigation was permissible under IPP 10.1(e). The agency's collection of personal information in the personnel and related files was for the purpose of administering C's employment. As the contractor was engaged to investigate complaints about C's working conditions, the use was "directly related" to the administration of C's employment: *N v Commonwealth Agency* [2009] PrivCmrA 17.

Health services

[7.2582] Examples of "directly related" secondary purposes within reasonable expectations in the context of a health service provider will generally include (*GPPHS* pp 14-15; *DNPPG* p 70):

- a health service provider collects health information about an individual for the purpose of providing treatment, and then decides, for ethical and therapeutic reasons, that they cannot treat the individual. The provider advises another heath service provider at the medical clinic of the individual's need for treatment and of the provider's inability to provide that treatment. This disclosure to the other provider is directly related to the purpose for which the information was collected, and would be within the individual's reasonable expectations (*APPG* at [6.27]);
- locating a patient's address in order to make a home visit;
- informing an individual about available products or treatments (eg a naturopath informing a customer of a new and superior herbal product that the customer could benefit from using;
- informing a patient about bodies, groups or organisations that may assist him or her in recovering from an illness or addiction (eg a support group or helpline).

The Commissioner has indicated that, for the purposes of the exemption under APP 6.2(a), "directly related purposes include many activities or processes necessary for the functioning of the

health sector" and provided the following examples (OAIC, *Business resource: Using and disclosing patients' health information* (2015) (DRAFT)):

- use or disclosure for a provider's management, funding, complaint-handling, planning, evaluation and accreditation activities (eg to assess the cost effectiveness of a service);
- disclosure to a medical expert for a medico-legal opinion or an insurer, a medical defence organisation or a lawyer for the purpose of addressing liability indemnity arrangements (such as reporting an adverse incident) or for the defence of anticipated or existing legal proceedings;
- disclosure to a clinical supervisor by a psychiatrist, psychologist or social worker.

The use of health information for activities such as staff training, fundraising and disclosures to the media is unlikely to be considered to be a directly related secondary purpose (*GPPHS* pp 16-17). Where information is intended to be used for such purposes, it should be de-identified or the individual's consent should first be obtained.

Where a health service provider needs to share a patient's health information on a need-to-know basis with other members of a treating team, the Commissioner has confirmed that this will generally be permitted under APP 6.2(a) where the patient has been informed that such disclosures may take place on the basis that it is within reasonable expectations and for a directly related purpose. The Commissioner has provided the following guidance (OAIC, *Business resource: Using and disclosing patients' health information* (2015) (DRAFT)):

> If a patient's information is likely to be shared within a treating team, you should tell the patient that such disclosures may take place. You should also tell the patient who is in the treating team (such as a GP, physician, physiotherapist and others), and how much information may be disclosed to particular members of the team. A patient may be sensitive about certain information being shared without their consent even across a treatment team, or with particular members of it.
>
> While information can be shared with consent ... consent will generally not be required where effective communication has established a clear, shared understanding between the provider and the patient about the likely uses and disclosures that may occur as part of their treatment.

Sale of business and due diligence

Related materials
- OPC, *Information Sheet (Private Sector) 16 - 2002: Application of Key NPPs to Due Diligence and Completion when Buying and Selling a Business*

[7.2583] Disclosure by a vendor organisation to a potential purchaser of personal information (eg information about business contacts, trading partners, suppliers, associated offices, debtors, client blacklists) during due diligence will, in most cases, be directly related to the primary purpose of collection (to enable the continued or future provision of the relevant product or service) and be within the individual's reasonable expectations (OPC, *Information Sheet (Private Sector) 16 - 2002: Application of Key NPPs to Due Diligence and Completion when Buying and Selling a Business* at pp 2-3). However, the vendor is expected to place appropriate restrictions on the potential purchaser regarding how it may handle the information during the due diligence process.

For commentary on vendor's obligations during due diligence, see [165.19].

Generally, a vendor organisation will be permitted to disclose personal information held by it to a purchaser of its business where the purchaser continues to provide the same type of goods or services and does not change the nature of the business as this will generally be deemed to be for a related purpose and within the individual's reasonable expectations (OPC, *Information Sheet 16*). This will include information about such things as customer files, commercial transactions entered into with other entities, tenants of rental properties and key office holders in supplier organisations (OPC, *Information Sheet 16* at p 5).

For commentary on transfer of a business, see [165.40].

[7.5000] Australian Privacy Principle 11—security of personal information

Related materials
- Data security – commentary and practical guidance at [205]
- OAIC, *Guide to securing personal information* (2015)
- OPC, *Information Sheet 6 – 2001 Security and Personal information*
- RACGP, *Computer security guidelines: A self assessment guide and checklist for general practice* (3rd ed)
- OICQ, *Information sheet – Personal information and network security – lessons from the Auditor-General's report*
- OVPC, *Guidelines to the IPPs* (3rd ed, 2011) at pp 97-118 (under "IPP 4: Data security")
- *AS/NZS ISO/IEC 27001:2006 Information technology – Security techniques – Information security management systems – Requirements*
- *AS/NZS ISO/IEC 27002:2006 Information technology – Security techniques – Code of practice for information security management*
- *AS ISO 15489.1 – 2002 Records management – General*
- *AS ISO 15489.2 – 2002 Records management – Guidelines*
- Commentary on cloud computing (including data security issues) at [150]

Overview of APP 11

[7.5005] APP 11 requires an entity to take reasonable steps to protect personal information against misuse, interference, loss and unauthorised access, modification and disclosure. It also generally requires entities to destroy or de-identify information once it is no longer required.

APP 11 applies to information that an entity "holds". The term "holds" extends beyond physical possession of a record to include a record that an entity has the right or power to deal with (eg records held in an off-site third-party storage facility) (*APPG* at [11.5]).

Comparison with former NPPs and IPPs

[7.5006] APP 11.1 differs slightly from data security requirements that existed under NPP 4 ("Data security") and IPP 4 ("Storage and security of personal information") in that it requires personal information to be protected against "interference" (the meaning of the word is discussed at [7.5090]), a term to which neither NPP 4 nor IPP 4 referred.

For private sector organisations, data security obligations under APP 11 are almost identical to those that existed under NPP 4. APP 11.2 differs slightly from NPP 4.2 in that it expressly provides that an organisation is not required to destroy or de-identify personal information if it is required to

retain the information by law. This was, however, permitted under NPP 4.2 by virtue of the fact that retention of information to meet a legal obligation amounted to a need to use the information.

For agencies, obligations under APP 11.1 closely reflect those that existed under IPP 4. However, obligations under APP 11.2 to destroy or de-identify personal information in relation to which an agency no longer has any use had no equivalent under the IPPs. As such, APP 11.2 imposed new obligations on agencies in regard to records retention.

Data security – commentary and practical guidance

[7.010] Detailed commentary on data security issues is set out at [205], including on:

- what constitutes "reasonable steps" to secure information (at [205.20]);
- relevant security standards (at [205.30]);
- checklist of data security risks and control measures (at [205.40]);
- portable storage devices, such as laptops and USB flash drives (at [205.70]);
- data security breaches and notification (at [205.85]).

[7.5058]

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

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

"Such steps as are reasonable in the circumstances"

[7.5080] What are reasonable steps to secure information will depend on the circumstances. For detailed commentary on what constitute reasonable steps to secure information, see [205.20] (in the "Data Security" chapter).

In relation to what constitutes reasonable steps to secure information in the context of data stored by a cloud service provider, see [150.10].

"Misuse", "interference" and "loss"

[7.5090] It is a "misuse" of personal information if the information is used by an entity for a purpose that is not permitted by the Privacy Act (*APPG* at [11.11]).

An "interference" with personal information occurs where there is an attack on personal information that interferes with the information but does not necessarily modify its content. For example, this may include an attack on a computer system that leads to exposure of personal information (*APPG* at [11.13]).

A "loss" of personal information can include a physical loss or an electronic loss (*APPG* at [11.14]).

Cases

Contents

Unauthorised staff access

[7.5400] The Privacy Commissioner commenced an own motion investigation into Vodafone Hutchison Australia following media reports that billing and call records for up to four million customers were available on a publicly accessible website with low levels of security protection. Vodafone used "store logins" (ie shared logins) and shared passwords to restrict staff access to the application in which customer information was stored. Further, staff access to information, including full identity document information such as passport numbers and expiry dates, was not restricted on a need-to-know basis. *Outcome:* There was no evidence to support the media reports that personal information was available on a publicly accessible website. However, the use of store logins and the availability of full identity information to all application users meant that Vodafone did not have appropriate data security measures in place and, as such, breached NPP 4.1. Vodafone's business model included licensed dealerships which carried underlying data security risks. Such risks warranted additional security safeguards being taken, such as appropriate authentication of remote users and the use of individual, rather than store, logins. Vodafone made changes to its security systems, reviewed staff access levels, reviewed whether identity document information could be masked and issued individual login IDs and passwords to all staff in stores: *Own motion investigation report, Vodafone Hutchison Australia* (OAIC, 2011.

The applicant, a college student, complained that the respondent had failed to properly secure information contained in counselling files, resulting in the information being used for purposes unrelated to the counselling. The respondent held its counselling files within its Counselling and Careers Service in a filing cabinet. The filing cabinet was locked, the key to it securely stored, each night. The entrance to the office was locked, with access restricted to counselling staff. Only counselling staff had access to client files. *Held:* The respondent had taken reasonable steps to secure the information in accordance with s 12(c) of the *Privacy and Personal Information Protection Act 1998* (NSW) and sch 1, cl 5(1)(c) of the *Health Records and Information Privacy Act 2002* (NSW): *JT v Technical and Further Education Commission (No 2)* [2011] NSWADT 291.

MH was formerly employed as a legal officer of the respondent agency. The agency had collected MH's CV and MH's job application for managing MH's employment issues (employee files). Documents provided with the complaint included MH's affidavit and MH's employee files. MH was later dismissed by the agency and MH commenced proceedings in the Supreme Court for unfair dismissal. During those proceedings, the agency's Legal Services Branch (LSB) Manager provided copies of the employee files to the Supreme Court registry. A complaint was also lodged by ND, another agency employee, about MH with the Office of the Legal Services Commissioner (OLSC) alleging that MH had deposed and sworn a false affidavit. The LSB Manager also lodged complaints with the Registrar of the Supreme Court and the OLSC alleging that MH had perjured himself in an affidavit and attached the employee files to the complaints. The employee files had been provided by the agency's Human Services division to the agency's Deputy General Counsel for staff management purposes and then emailed to the LSB Manager's personal email address. The LSB Manager then attached copies to her letters of complaint. The case involved a complex series of events and facts, however, a key issue was how the LSB Manager came into possession of the

[108]

Practical issues and privacy solutions

[114]

Privacy compliance plan

Related materials
• PrivacyNSW, *A Guide to Making Privacy Management Plans* (2012)

[114.10] A privacy compliance plan (sometimes referred to as a privacy management plan) sets out control measures an entity will adopt to minimise and manage privacy risks and to meet compliance obligations under applicable privacy principles. Control measures will generally comprise information management policies, procedures and systems. A plan assists in providing an organisation-wide, structured approach to privacy compliance.

Development of a compliance plan generally needs to be preceded by a privacy audit in order to ascertain, for example, what personal information the entity holds, the purposes for which the information is used and disclosed and measures that need to be taken to ensure compliance.

Key privacy control measures that should be addressed when developing a privacy compliance program are set out below.

Control measure	Purpose	Commentary
Privacy collection notices	To meet notification requirements	at [123.10]
Privacy consents	To ensure necessary privacy consents are obtained through, for example, terms of service, privacy consent forms and privacy collection notices	at [126.10]
Privacy policy	To meet transparency requirements regarding data management practices and to assist in obtaining privacy consents (express or implied, depending on whether they are incorporated into contractual terms)	at [117.10]
Collection forms	To meet collection requirements (primarily ensuring they do not request unnecessary information, including identity details if it is lawful and practical to deal anonymously, and that they contain necessary privacy collection notices)	at [7.998] (regarding APP3)
Internal information management policies	To ensure personal information is used, disclosed, stored and otherwise handled by staff on a day-today basis in accordance with privacy law requirements. These should cover steps for verifying identity and the authority of third party authorised representatives to act on behalf of individuals.	n/a
Procedure manuals and guidelines	To assist in the implementation of internal policies in the context of specific processes (eg guidelines might set out common requests by individuals for disclosures of personal information along with sample responses)	n/a
Information systems design	Information systems should be designed and/or adjusted to ensure that information handled within them is done so in accordance with privacy law requirements	n/a
Data security and destruction policies	To assist in meeting data security obligations	at [205]
Document retention policy	To assist in determining periods for which records and information should be retained prior to destruction	at [7.5618]

[117]

Privacy policies

- what will happen if the organisation determines that a child does not have sufficient capacity to exercise his or her rights (eg the organisation may allow the child's parent to exercise the child's rights);
- any other special measures that apply in relation to children (eg an organisation may have a policy of destroying information about a child if requested to do so by a parent, although there is no legal obligation to do so).

Sample privacy policies

[117.30] Sample privacy policies are set out below. A privacy policy must accurately reflect the relevant entities' *actual* information handling practices. Accordingly, the sample policies below should be used as templates, or starting points, only and adapted accordingly.

Sample privacy policy

We are committed to protecting the privacy of individuals' personal information in accordance with the *Privacy Act 1988* (Cth). This document outlines how we collect, use, disclose and otherwise handle personal information.

Collection and use of personal information

We collect the types of personal information outlined below for the reasons and in the ways indicated:

- Customer sales information – We collect personal information about individuals when they purchase goods and services from us, including in person, over the phone and through our website. This information may, for example, include name, address, age, phone number, email address, credit card details and items purchased or services provided. This information is used to transact sales and to provide the goods and services ordered. Elements of the information may also be used for market research purposes and to inform customers about new products and services. When you ring us, we may also record phone conversations with your consent for quality review purposes.
- Credit history information – We conduct credit history checks with credit reporting agencies as part of our credit application assessment process.
- Loyalty club member details – This information includes details such as name, address, age, phone number and email address and is collected primarily through membership application forms. We also collect personal information through member survey forms in which we ask members to provide details about a range of issues relating to their interest goods, services and the club. Information about members is used to administer membership accounts and to develop and inform members about club events, offers and promotions and our products and services.
- Competition entrant details – From time-to-time we conduct competitions and collect personal information about entrants provided on entry forms, such as name, address, phone number and email address. This information is used for conducting the competitions and to send entrants information about our products and services.
- Website – We collect personal information when individuals communicate with, or purchase products from, us through our website, such as name, email address, items purchased, credit card details and details provided in messages. Payment details provided through our website are processed through a secure web server with strong encryption. We collect de-identified statistical information about our website visitors through the use of sessional cookies to evaluate our website performance, such as the number of visitors, pages viewed, types of transactions conducted, time spent on the website and documents downloaded. This data does not, however, enable us to identify individuals.
- CCTV – We record CCTV footage of public areas within our stores and offices.
- Customer complaints – This information may include name, address, phone number and complaint details and is used for complaint handling purposes.
- Recruitment information – We collect information about job applicant for the purpose of assessing their suitability for employment. This may include any information relevant for this purpose, such as employment history, education, training, qualifications, salary and reference information from referees.

Any information we collect may also be used for purposes directly related to carrying on our business, such as quality audits, risk management, staff training and product development.

If you would like any further information about how we handle personal information, please lodge a request with our Privacy Officer whose contact details are provided below.
Privacy Officer
Organisation Pty Ltd
1 Organisation Road, Sydney NSW 2000
Phone: (02) 1234 5678
Facsimile: (02) 2345 6789
e-mail: privacy@organisation.com.au

Last updated: [*insert date*]

Sample privacy policy – Health service provider

We are committed to protecting the privacy of our patients' health information in accordance with the *Privacy Act 1988* (Cth). This document outlines how we collect, use, disclose and otherwise handle personal information.

How we collect your information

We primarily collect information about you through correspondence that we engage in with you; for example, during a consultation or telephone conversation or from information that you include in a letter, registration form or email.
We only collect information in a manner that is reasonable and, to the extent possible, that is not intrusive. We hold all consultations in private rooms to ensure that, where you provide information verbally, you cannot be overheard. Staff members are not permitted to enter a consultation room without first knocking and being given permission to enter. Further, if a staff member other than the treating practitioner (or practitioners) is present during a consultation, you will only be requested to provide information if you have consented to the staff member being present.
We may collect information about you from persons or sources other than yourself. However, we will only do this with your consent, or, in the case of an emergency during which you are unable to provide consent, where it is necessary in order to treat you. Other sources from which we may collect information about you include treating specialists, family members, friends, employers and hospitals in which you have been treated.

Types of information we hold about you

We only hold information about you if it is relevant to providing you with a health service. Such information generally includes your name, contact details, payment details, records of correspondence, billing statements, general practitioners that you have attended, next of kin, health insurance details and medical records. Medical records may contain information about symptoms, prescriptions, medication, family medical history, test results, diagnoses, occupation and travel details.
As we provide health services to children, some of the information we hold relates to young people.

How we hold your information

Depending on the circumstances, we may hold your information in either hardcopy or electronic format, or both. Generally, notes made during consultations are held in hard-copy format and later re-created in electronic format. We hold a hard-copy of all correspondence entered into. All hard-copy documents are held in an on-premises compactus. All electronic records relating to you are maintained in your electronic medical file on our computer network. Information on the network is not placed on, or accessible from, the internet.

How we use your information

We use your personal information and health information:

- to provide you with health services now and in the future;
- to process your registration;
- for internal purposes such as procedural assessments, risk management, product and service reviews, staff training, accounting and billing;
- to make follow-up calls, where it is appropriate to do so, after we have provided you with treatment;

[126]

Consent

Sample privacy consent form

I give my consent to ABC Company ("you", "your") handling my personal information in the ways indicated below:

- to collect health information about me that is relevant to assessing my application from any health service provider, and I authorise any such health service provider to disclose such information to you for this purpose;
- to use my personal information for product research and development purposes, including conducting customer surveys;
- to disclose my personal information to related entities within the ABC group of companies for application assessment purposes.

Name: .....

Signed: .....

Date: .....

Identifying collections, uses and disclosures that require consent

Overview

[126.105] Data management practices for which an entity should obtain privacy consents could be described as generally falling within three broad categories; namely, consents for:

- collections of sensitive information for which consent is required (see [126.12]);
- uses or disclosures which are only permitted with consent (ie uses or disclosures that are not otherwise authorised under privacy principles) – these will generally always be secondary uses and disclosures (ie uses and disclosures for purposes other than the primary purpose of collection) as privacy statutes permit use and disclosure for the primary purpose of collection;
- uses or disclosures which are, or are likely, permitted under privacy principles but in relation to which it is preferable to obtain consent, either:
    - as a matter of good privacy practice (eg to ensure information is handled in accordance with individuals' wishes, regardless of any statutory authority permitting such practices – see [126.10]); or
    - for risk minimisation purposes (eg for certainty where there is a risk that a provision that seemingly authorises a use or disclosure without consent could be interpreted in a contrary manner).

In order to identify specific collections, uses and disclosures for which an entity should obtain consents, it will often be necessary to map the entity's data flows (see [133.30]). This enables the entity to document what personal information it holds and the purposes for which it is used and disclosed which, in turn, enables identification of collections of sensitive information and secondary uses and disclosures of personal information for which consent is needed. These steps are commonly undertaken as part of a privacy audit (see [133]).

Often, privacy consent forms and clauses are drafted to seek consent for collections, uses and disclosures that are clearly authorised under privacy legislation without consent (see [126.08]). This can cause forms and clauses to be unnecessarily lengthy, resulting in poor communication and notification where individuals avoid reading them. For this reason, it is sometimes preferable to avoid requesting such consents, particularly where they relate to low risk practices or non-sensitive information, and, instead, to outline the relevant practices in privacy collection notices or privacy policies.

Where information relates to more than one individual, the consent of each person concerned is needed. For example, if an entity requires consent to use or disclose a document that relates to a married couple, consent from both the husband and wife will be necessary. The entity should not assume that, because one spouse consents, the other does as well.

Checklist

[126.106] The fact that not all collections, uses and disclosures require consent can make the process of identifying which consents an entity should obtain difficult. A checklist to assist in this process is set out below. A template table to assist in recording and analysing the information is set out at the end of the checklist.

- ***Map data flows*** – In order to know what personal information is held, map the data flows (for guidance on how to do this, see [133.30]) that fall within the scope of the review (this could, for example, range from a limited number of data flows relating to a specific activity or all data flows within an entity) and allocate each set of information associated with a particular process a data set name, eg sales order data.
- ***Identify purposes of uses and disclosures*** – For each data set, identify and record:
  - the primary purpose of collection;
  - the purpose(s) for which it is used;
  - the purpose(s) for which it is disclosed and to whom;
- ***Identify entities to be covered by consents (if multiple entities)*** – Where a standard consent form is being drafted for use by several entities, identify and record each such entity.
- ***Identify privacy statute(s) to which entity(ies) are subject*** – Identify which privacy statute(s) (or administrative instructions) apply to each entity (*note:* contractors for federal or State government agencies may be bound by public sector privacy laws – see, eg, at [45]).
- ***Record whether data falls within a sub-category of personal information*** – Identify and record whether any information contained within a data set falls within a sub-category of personal information, as defined within applicable statute(s) (eg "health information" or "sensitive information"), in order to know whether additional rights or obligations apply to the information by virtue of its classification within the relevant sub-category.
- ***Identify consents required for collection*** – For each data set, identify whether consent is, or is not, required for collection under the applicable privacy statute(s) (or administrative instructions) having regard to, for example, the primary purpose of collection and purposes for which it is used or disclosed (eg consent may be required to collect sensitive information or to use personal information for a particular secondary purpose).
- ***Identify consents required for relevant uses or disclosures*** – For each data set, identify whether consent is, or is not, required for each purpose for which the information is used or disclosed under the applicable privacy statute(s) (or administrative instructions) (eg consent generally will not be required where a data set is used for the primary purpose of collection but may be required to use it for a secondary purpose or, where it contains health information, to disclose it to a Commonwealth agency under HPP 14 of the *Health Records and Information Privacy Act 2002* (NSW)).
- ***Identify any non-essential consents desired to be obtained*** – For data sets for which consent is not required, determine whether the entity wishes nevertheless to obtain consent as a matter of good privacy practice or for risk minimisation purposes.
- ***Identify any implied consents to be relied upon in lieu of written consents*** – For each data set for which consent is necessary, or is nevertheless to be obtained, determine whether the entity will obtain written consent or, if possible and appropriate, will instead rely on implied consent (and therefore not obtain written consent).
- ***Identify any additional consent options to be provided*** – Consider whether any additional consent options will be provided to individuals; for example, to enable individuals to opt-out

[132]

Access and correction

Related materials
- OICQ, *Information sheet - Evidence of authority and identity*
- Commentary on access under APP 12 ("Access to personal information") at [7.6000]
- Commentary on access under APP 13 ("Correction of personal information") at [7.6500]

[132.10] Privacy principles and other provisions under privacy legislation generally provide individuals with rights to access and correct personal information an entity holds about them (see, eg: Cth - APPs 12 and 13; ACT - TPPs 12 and 13; NSW - IPP 7, 8; NT - IPP 6; QLD - IPP 6, 7; SA - IPP 5, 6; Tas – PIPP 6; Vic - IPP 6). There is a large variation in the number of requests for access and correction that entities receive, often depending on industry. For example, health service providers tend to receive a large number of such requests, where as many businesses (even large corporations) receive few, if any, such requests.

Entities, particularly those that receive regular requests for access and correction, should have in place procedures and forms for the lodgement and processing of request for access and correction.

Privacy principles relating to access and correction generally set out various grounds on which an entity is entitled to deny a request for access or correction. Once a request has been lodged, an entity should have in place a process whereby it is vetted to see if, firstly, there is any reason as to why the entity may wish to refuse the request and, if so, to assess whether any exemptions can be relied upon to deny the request.

Where fees are charged for processing requests for access, applicants should be notified of the fees prior to processing of the application.

For commentary relating to the provision of access and correcting records under APPs 12 and 13 of the Privacy Act, see [7.6000] and [7.6500] respectively.

Sample forms for requests for access and correction are set out below.

Sample form: Request for access

Request for access to personal information

Privacy notice. We will use the information you provide to process your request for access. We may disclose the information to any third parties involved in providing you access, such as courier service providers. If you do not provide the information requested on this form, we may be unable to process your application. You may request access to the information we collect about you at any time.

Applicant's details
Title: Mr/Mrs/Miss/Ms
First name: .....
Surname:.....

You must provide evidence of your identity.

Agents/authorised representatives
If an agent or other authorised representative is requesting access on behalf of the applicant (eg solicitor or family member), the representative must provide the details below.

Title: Mr/Mrs/Miss/Ms
First name: .....
Surname:.....
Relationship with applicant: .....

You must provide:
- evidence of your identity; and
- proof of your authorisation to act on behalf of the applicant, eg written and signed authorisation, letter of engagement or power of attorney.

Contact details
Please provide contact details for the medium of communication by which you wish to be contacted.

Address: .....
Post code: .....
Telephone: .....
- business hours:.....
- non-business hours:.....

Fax: .....
Email: .....

Request for access
I hereby request that you provide me with access to (tick applicable box):

☐ all personal information held about me; or
☐ the following documents containing personal information about me:
.....
.....
.....

☐ any documents containing the following types of personal information about me:
.....
.....
.....

Signature **Date**

....

Please send this completed form to:
Privacy Officer
[*insert mailing address*]

[138]

Outsourcing

Contractual measures

Introduction

[138.58] An outsourcer should take contractual measures with a contractor to ensure personal information accessed or handled by the contractor is handled and secured appropriately by the contractor. Whilst a brief clause solely requiring compliance with the Privacy Act should, in the event of a breach of the Act by the contractor, provide the outsourcer with a legal remedy (being action for breach of contract) to address any subsequent losses it suffers (in the absence of which, only affected individuals may have an avenue of redress, namely, to lodge a privacy complaint), contractual terms should address in detail specific practices and standards that must be met by the contractor when handling the relevant personal information.

The extent to which terms can be negotiated will often depend on various factors, such as the bargaining power of each party, duration and value of the services or contract (eg once off provision of services versus a long term contract), amount and sensitivity of information being handled and whether information is held in encrypted form.

Entities should, as a matter of standard procurement procedures, require contracts with service providers involved in the handling of personal information to be legally vetted to ensure appropriate privacy terms are incorporated into the agreements. A surprisingly large number of organisations, including even large data storage service providers, still do not have privacy terms in their standard terms of service. An outsourcer should insist on the inclusion of such terms where appropriate. Existing contracts should, where possible, be varied to incorporate such terms.

A checklist of key issues that should be considered and, where relevant, addressed in agreements with contractors is set out below. In some instances, it will be appropriate to integrate privacy clauses with other "non-privacy" clauses as the matters they address are not always unique to privacy, eg issues relating to confidentiality, ability to subcontract, data security and termination for breach.

Checklist: privacy issues to address in contracts

[138.60] A checklist of key issues that should be considered and, where relevant, addressed in agreements with contractors is set out below.

Issues commonly addressed by privacy terms in contracts include:

- ***Compliance with privacy laws and standards*** – The service provider should be required to comply with relevant statutes (eg Privacy Act, health records statutes and *Spam Act 2003* (Cth)) regarding the manner in which it handles personal information in order to provide a contractual remedy for any breaches of the legislation. If the service provider is not bound by a relevant statute (eg the Privacy Act because it is a small business operator), the contract should provide that the service provider must comply with the relevant Act as though it were bound by it.

  The service provider should also be required to comply with any additional information handling requirements, standards or policies (eg information management and IT security policies) the principal wishes to impose on the service provider. These may relate to information management practices generally or specific elements of them (eg staff training requirements).
- ***Collection*** – If the service provider collects personal information on behalf of the principal, the service provider should be required to provide any privacy notices to and obtain any privacy consents from individuals as reasonably required by the principal.
- ***Use*** – The purposes for which the service provider can use the personal information should be restricted to, for example, use solely for providing the services, unless the principal approves otherwise.

Sample privacy clauses

Related materials
- Australian Government Solicitor, *Legal Briefing (No 63) – Outsourcing: Agency Obligations under the Privacy Act (2002)* (containing sample contractor clauses for Commonwealth agencies)

[138.60A] Sample privacy clauses for a private sector entity bound by the *Privacy Act 1988* (Cth) are set out below. The clauses should be adapted to suit specific circumstances and requirements.

[**NOTE: Privacy issues should be addressed in conjunction with other contractual issues since they are not all unique to privacy compliance, eg confidentiality, subcontracting, data security and termination for breach. Accordingly, privacy clauses should be integrated with other terms of the agreement*]

1 Definitions and Interpretation

1.1 In this Agreement:

…

"Personal Information" means personal information as defined in the *Privacy Act 1988* (Cth) that:

(a) is held by the Principal (eg on its IT network or in hard copy documents) and accessed by the Service Provider; or

(b) is otherwise collected, generated, acquired or accessed by the Service Provider for the purposes of, or otherwise in connection with, the Services, including without limitation information that is collected from a third party or supplied to the Service Provider by the Principal.

…

"Services" means the services to be provided by the Service Provider pursuant to this Agreement.

[**NOTE: The terms "Principal" and "Service Provider" should be defined to mean the relevant contracting parties*]

2 Privacy

Compliance with privacy laws and standards

2.1 In relation to collecting and handling the Personal Information, the Service Provider must comply, and cause its officers, employees, agents and subcontractors (eg through contractual undertakings) to comply, with:

(a) the provisions of the *Privacy Act 1988* (Cth) or any applicable privacy code approved under s 18BB of that Act or, if the Service Provider is not bound by the *Privacy Act 1988* (Cth), the provisions of that Act as though it were bound by the Act; and

[**NOTE: If the Service Provider is not bound by the Act, the Principal could require it to opt-in to coverage of the Act under s 6EA of the Act*]

(b) any additional information handling requirements, standards and/or policies required to be complied with under this Agreement.

[**NOTE: List here, in particular, any Principal policies that must be complied with when accessing Personal Information held by the Principal, eg Information Security Policy*]

[**NOTE: If the Service Provider will be handling health information or information for marketing purposes, it may be appropriate to also require it to comply with applicable health records statutes and marketing laws*]

2.2 In relation to collecting and handling the Personal Information, the Service Provider must not engage in any act or practice that would constitute or result in a breach of the *Privacy Act 1988* (Cth) if the act or practice was engaged in by the Principal.

[205]

Data security

Reasonable steps to secure information

Related materials
- OAIC, *Guide to securing personal information* (2015)
- **[7.5400]** Data security breaches - Cases

[205.20] What will constitute reasonable steps or safeguards to secure personal information will depend on the circumstances. It is a subjective test based on the particular risks within the relevant organisation: *Own motion investigation report, Vodafone Hutchison Australia* (OAIC, 2011).

Data security measures must be continuously reviewed to ensure their effectiveness. In the context of the digital environment, the Commissioner has indicated that there is no "set and forget" solution to security and privacy as the environment is constantly evolving due to, for example, new vulnerabilities and changes in software programs and platforms: *Telstra Corporation Limited: Own motion investigation report* [2014] AICmrCN 1. Similarly, obligations will not be satisfied if an entity has adequate security measures in place to protect information stored on one of its systems, but does not implement these measures on other systems which also hold personal information: *Adobe Systems Software Ireland: Own motion investigation report* [2015] AICmrCN 1. There is often a risk of this occurring where, for example, an older system is being kept as a back-up or which is soon to be decommissioned. Such systems must still be appropriately protected, regardless of such factors.

Implementation of data security measures in the digital environment requires the involvement of IT staff as they are best placed to readily identify areas of risk based on their technical knowledge of how systems are structured and operate. It can be difficult, if not impossible, for legal and risk managers to identify or monitor for such risks other than by requiring IT security audits be undertaken. In contrast, IT staff who have a detailed knowledge of privacy obligations are well positioned to identify such risks in the course of their day-to-day activities if they have otherwise not been detected. Accordingly, IT staff should be required to undergo privacy training with a view to ensuring they are able to identify privacy issues and risks in the course of their work, particularly when selecting settings for new software and hardware and designing new systems. This became particularly evident in breaches suffered by the telecommunications company, Optus, which led to it agreeing to an enforceable undertaking with the OAIC (see *Singtel Optus: enforceable undertaking* – case summary at [24.86]).

The OAIC has provided detailed guidance on reasonable steps that entities are expected to take under the Privacy Act to protect personal information in its *Guide to securing personal information* (2015). The guidelines indicate that what constitutes reasonable steps to ensure information security under the Act will depend on the circumstances. Relevant considerations will include (*APPG* at [11.7]; *GSPI* at p 12):

- the sensitivity and amount of the information;
- the nature of the entity (eg size, resources and business model) – for example, steps required of an entity that operates through a franchise will differ from those required of a centralised entity;
- possible adverse consequences if the information is not secured (this will usually depend on the nature of the information;
- whether data management is outsourced to third parties and whether they are bound by the Privacy Act;
- practicability (eg excessive time and cost involved) – however, the fact that it is inconvenient, time-consuming or imposes some cost is not in itself sufficient to warrant not taking any steps;

- privacy invasiveness of the security measures (ie if the measures are themselves privacy intrusive, such as requiring extensive personal information for ID verification, an appropriate balance must be found).

In earlier guidance materials, the federal Privacy Commissioner indicated that relevant considerations in determining reasonable steps will generally include (see, eg, OPC, *Guidelines to the NPPs* (2001) at pp 44-45):

- foreseeable risks;
- likelihood of risks eventuating;
- the level of sensitivity or confidentiality of the information (this will be one of the most influential factors – the more sensitive or confidential the information, the more significant will be the steps required to secure it);
- existing security measures (if there is already a high level of security, it may not be necessary to take any further steps);
- the frequency with which information is handled by the organisation (if it is used on a daily basis by a large number of employees, the need for increased security levels will be higher than if it is only used on occasion by a limited number of staff);
- the commercial or other value of the information (if the information is much sought after, the risk of unauthorised access will be greater);
- the privacy consequences and potential harm that may result from a breach of security (the more serious the consequences, the more likely it will be necessary to secure the information); and
- the size of the organisation and cost of security measures (a large organisation will generally be expected to invest a more significant amount of resources into establishing security measures than a small organisation due to the increased number of security risks that is likely to exist).

The Commissioner will have regard to security standards in determining whether reasonable steps have been taken to secure data – see [205.30].

Reasonable steps must include both documented policies and procedures and behaviours consistent with those policies and procedures. In other words, policies and procedures in and of themselves do not demonstrate compliance with data security obligations if it cannot be shown that organisations are acting on them: *Telstra Corporation Limited: Own Motion Investigation Report* (June 2012).

Where an entity is requested by a third party to disclose personal information about an individual (eg a police officer), the entity is expected to have regard to any professional obligations (eg a professional code of conduct) and to ask the reasons for the request. Such steps are a necessary part of securing the information from unauthorised disclosure: *'EZ' and 'EY'* [2015] AICmr 23 at [79].

Large corporations and public sector agencies have available to them dedicated resources in the form of intrusion detection systems, sophisticated firewalls, IT security staff and chief information and technology officers. This entitles the community to expect from them higher rates of awareness of information security risks and vigilant breach prevention programs than in relation to small businesses and individuals: *Own Motion Investigation,* Privacy NSW (June 2011).

A data security breach resulting from an isolated human error will not necessarily mean an organisation has failed to take reasonable steps to secure data where it can show that it had in place appropriate data security controls. In 2010, a mailing list error by the respondent telecommunications company, Telstra, resulted in approximately 60,300 letters with incorrect addresses being mailed out. In an investigation report, *Telstra Corporation Limited: Own Motion Investigation Report* (7 July 2011), the Commissioner found that Telstra had a range of security measures in place to protect customer personal information involved in mail campaigns, including privacy obligations in agreements with mailing houses, privacy impact assessments at the outset of mail out initiatives and procedures to ensure staff handle personal information appropriately during mail campaigns. The Commissioner found that the incident occurred as the result of a one-off human

Checklist: Data security risks and control measures

[205.40] The tables below provide checklists of key areas of data security risk that should be reviewed, and guidance on relevant control measures, when conducting a data security review for the purposes of assessing compliance with data security obligations under privacy laws. The checklist addresses key areas of risk only to the extent that they directly relate to protecting the privacy of personal information (data security, as an area of risk management, protects a broader range of interests than just privacy – see [205.10]). Accordingly, the checklist does not address all data security issues that, for example, would commonly be covered in a comprehensive information security plan. Rather, it focuses on key areas of risk to the extent they are relevant to assisting in compliance with privacy laws. The checklist has been developed based on:

- relevant parts of Australian Standards pertaining to information security and records management;
- data security guidelines published by the Privacy Commissioner;
- data security issues which, in practice, have led to privacy complaints being lodged the with the Privacy Commissioner against entities; and
- fundamental security controls that the Privacy Commissioner would generally expect a large entity to have in place (based on case notes published by the Commissioner).

Hardcopy and electronic records

Issue	Guidance
Information security policies	Entities should establish and implement information security policies that appropriately address data security risks. This can be done through an overarching Information Security Policy covering both hardcopy and electronic records which references other documentation which may support the policy, eg more detailed security policies and procedures relating to specific practices or systems. In addition to an Information Security Policy, examples of policies through which data security risks are commonly addressed include: • Information Management Policy • IT Security Policy • Portable Storage Devices Policy • Electronic Records Disposal Policy • Password Policy • Remote Access Policy • Cryptographic Policy • Acceptable Usage Policy (Internet & Email) • Document Retention Policy

Governance/Information security responsibilities	Overall responsibility for information security should be assigned to one or more appropriately qualified and experienced senior officers (eg Chief Information Officer, Information Security Manager, Records Manager, Privacy Officer) or to a governing body or committee. Clear lines of authority for decisions regarding information security should be established.
Information classification	Appropriate policies (eg Information Security Policy) should classify information, including in particular personal information, into appropriate categories, such as "highly confidential", "confidential" and "public", and establish rules and procedures regulating how each category may be handled.
Employees	The following security measures should be taken in relation to employees: • employees should be required to comply with data security policies and procedures through employment contracts; • ensure job descriptions clearly specify data security responsibilities; • where appropriate (eg in relation to high risk data), have "job handover" notes address privacy issues; • where appropriate, background checks and police clearances obtained prior to allowing access to systems and information; • ensure employment contracts require employees to return all records containing personal data upon or prior to termination of employment (and ensure such term survives termination of the contract); • confidentiality/non-disclosure agreement covering personal data (including after termination of employment); • ensure policies are enforced regularly and consistently; • a formal disciplinary process should be in place for employees who have committed a security breach to ensure policies are enforced; • an appropriate policy should prohibit staff accessing, copying, modifying, using and/or removing personal data for any purpose other than a work purpose; • where appropriate, staff should be prohibited from handling customer matters where the customer is personally known to the staff member. In such cases, the customer should be referred or transferred to another staff member.
Contractors	Where contractors access or handle personal information on behalf of an outsourcing organisation, contractual measures should be taken to ensure the contractor meets appropriate privacy standards in regards to handling the information (for commentary on contractors, including a checklist of contractual measures to be considered for addressing in agreements, see [138.10]).
Reproduction	Policies should prohibit copying/digitising/distributing personal data in any format for any purpose other than a work purpose.

Monitoring and review	In view of the constantly and rapidly evolving nature of data security risks, a review program should be established for an organisation's information security program (eg policies, procedures, controls and systems) to ensure security policies and procedures are implemented, up-to-date and regularly tested and enforced. Review should include assessing ways to improve the organisation's information security program. Independent reviews should also be planned at regular intervals or when significant changes to the organisation's information security program or risks occur. Such reviews should be carried out by appropriately qualified individuals, such as information management and IT security specialists, independent of the area under review.

Hardcopy records

Issue	**Guidance**
Storage	Physical security measures prevent unauthorised access to information held in documents and are relevant to all forms of storage. Physical security measures include lockable drawers, lockable filing cabinets and compactuses, placement of filing cabinets in locked rooms, safes and lockable storage containers. The quality or security grading of storage facilities (eg of locking mechanisms and filing cabinets) should be higher for high risk documents. Whether it is appropriate to leave lockable facilities unlocked during business hours will depend largely on the sensitivity of the documents they contain – the more sensitive the documents, the more reasonable it will be to leave the facilities locked at all times. Where offices are open plan and there is no physical separation between departments, this will result in an increased need for lockable storage facilities to reduce the risk of non-departmental staff accessing documents without authority.
Access controls	Information management systems should incorporate procedural and physical access controls to ensure documents are protected from unauthorised access, modification and disclosure. Such controls should be used to ensure staff only access documents on a need-to-know basis having regard to their work functions. In addition to physical controls, procedural measures (which establish a disincentive of disciplinary action if breached) are of particular importance in the context of hardcopy documents as access logs are often impractical in relation to such records (unlike electronic records).
Clear desk policy	To reduce the risk of unauthorised access to documents during and outside business hours, a clean desk policy (requiring, for example, that documents not be left on unattended desks or that staff file documents away when leaving the office) should, where appropriate, be adopted in relation to documents containing personal information. The circumstances in which such a policy should be adopted, and its scope, will depend on factors such as the sensitivity of the documents, the risk of attempts at unauthorised access being made, the number of people who have access to desks (often a large number in open plan offices with no physical separation between departments) and practicality for staff.

Printing	To reduce the risk of unauthorised access to documents awaiting collection in printer trays, secure printing mechanisms should be used where appropriate. This entails, for example, a staff member selecting "Secure Print" in print properties when sending a file to print. This will require the staff member to enter a code through their computer. When at the printer, the staff member will be required to re-enter the code in order to print the file, enabling the staff member to remove the document from the printer tray as soon as the file is printed.
Transfer and communications	Security measures should be in place to protect documents and data whilst being transferred or communicated. Issues that should be addressed include: • *ID verification/user authentication* – verifying ID before discussing/disclosing/providing access to personal data (eg by requiring three pieces of identifying information over the phone, digital signatures via email) (in relation to user authentication, see [186.1005]); • *Authorised representatives* – verifying the authority of authorised representatives who can access account details on behalf of an individual and exercise their privacy rights, for example, by: o requiring account holders to list authorised third parties; o sighting an original power of attorney document to ensure an attorney is acting within the scope of his or her authority; o sighting a signed letter of engagement of a lawyer to ensure the lawyer is acting on behalf of an individual and also within the scope of his or her authority; and o adopting a call-back system whereby, if an authorised representative acting in an official capacity (eg an MP investigating a complaint by a constituent) calls to make an enquiry, the entity calls the caller back through their main office line; • *Offsite transfers* – requiring manager approval for transfer or taking off-site of high risk documents; • Where high risk documents, or large numbers of documents containing personal information (eg storage containers containing large numbers of customer files), are sent off-site using third party service providers, they should only be sent using reliable service providers and transferred by signed receipt delivery services (eg Australia Post's registered post service) or equally secure means (eg in person) to reduce the risk of them being lost in transit, intercepted and being delivered to incorrect recipients. In some instances, additional security measures may be appropriate; for example, use of locked containers and tamper-evident packaging. • Whilst use of signed receipt delivery services can significantly increase postage costs and be relatively time consuming (as it can, for example, require completion of forms – Australia Post offers a service for bulk lodgement of registered post items to avoid having to manually complete individual forms), investigations by the Privacy Commissioner (eg of a courier leaving surveillance reports in a public thoroughfare and of medical x-rays being lost in the post when sent by standard mail) indicate that organisations should use such services at least in relation to high risk documents. • Where appropriate, file movements off-site (eg movement of medical records off site to send to a relief practitioner or to a nearby hospital), including those between branch offices, should be monitored through logs recording the following details:

Portable storage devices

Related materials
- OPC, *Information Sheet (Public Sector) 3 – Portable storage devices and personal information handling*
- OVPC, *Use of Portable Storage Devices: A Guide to Policy Development* (2009)
- OICQ, *Information sheet – Portable storage devices and information privacy*
- AMA and MIIAA, *Clinical images and the use of personal mobile devices* (2015)
- OPCNZ, *Guidance Note on the Use of Portable Storage Devices*
- OVPC, *Portable Storage Devices: Privacy Survey* (2011) (contains detailed recommendations regarding steps organisations should take to secure portable storage devices)
- Government Services Division (Vic), *Information security – Use of portable storage devices* (2009)

Introduction

[205.70] A portable storage device (PSD) is any small, lightweight, portable device capable of storing and transferring large volumes of data (eg external hard drives, CDs/DVDs, USB flash drives, laptops, BlackBerries, MP3 players, smart phones and tablets). PSDs storing data pose a major data security risk by virtue of their portability and subsequent risk of being lost or stolen (particularly when taken off-premises), resulting in unauthorised disclosures.

In view of the extremely high data security risk posed by PSDs, arising by virtue of the fact that an entity's entire data holding can be stored on such devices, entities should, in addition to other IT security policies, adopt a portable storage device policy to specifically address and minimise risks posed by PSDs. In addition to improving security, this will assist in meeting data security requirements under privacy principles (Cth - APP 11; ACT - TPP 11; NSW – IPP 5; NT – IPP 4; QLD – IPP 4; SA – IPP 4; Tas – PIPP 4; Vic – IPP 4). For a checklist of issues that should be addressed in such a policy, see below at [205.75].

The federal Privacy Commissioner, Victorian Privacy Commissioner (OVPC) and Queensland Information Commissioner have each published guidelines regarding the management of PSDs and, in particular, the development of policies and procedures relating to the handling of PSDs and how to safeguard personal information stored on them. The AMA has also produced detailed guidance for doctors regarding the use of personal mobile devices to take clinical images (see the resources listed in the "Related materials" box above).

The Victorian guidelines were published following release by the Commissioner of findings of a survey it conducted into the Victorian public sector's use of PSDs (OVPC, *Use of Portable Storage Devices – Privacy Survey* (2009)). The survey showed that the public sector generally handled PSDs poorly and that their use of them potentially posed a serious data security risk. The report made 17 recommendations to assist agencies to comply with their privacy obligations in their use of PSDs (set out in Appendix 2 of the guidelines). The first recommendation was that, at a minimum, organisations need to have a formal policy on PSD use.

In May 2009, the federal Privacy Commissioner urged federal agencies to protect data on PSDs. This followed research conducted by the Commissioner which showed that, while most agencies had policies regarding the transfer of personal information, not all had appropriate controls covering the use of PSDs for the handling of personal information. Key findings from the research included:

- 75 per cent of agencies had policies covering the secure transfer of records to external parties, and 69 per cent had policies for staff temporarily working away from the office;
- 81 per cent had policies covering uses of agency-issued PSDs;
- 55 per cent had policies covering uses of privately owned PSDs;
- most agencies had controls to manage agency-issued PSDs, such as keeping a PSD register (97 per cent), requiring signed user agreements from staff (63 per cent), using minimum encryption standards (56 per cent) and providing staff training (63 per cent);
- 58 per cent had experienced the loss or theft of an agency-issued PSD within the past 12 months;

- 76 per cent allowed the use of private PSDs in the workplace, with agencies being more likely to use software controls (54 per cent) than hardware controls (16 per cent) to manage or restrict their use.

Checklist: Security risks and control measures

[205.75] A Portable Storage Device policy should apply to all PSDs and all users (including staff, contractors, consultants, interns, volunteers and visitors) and be flexible enough to apply to new types of PSDs.

Key issues that should be addressed in a Portable Storage Device Policy are outlined in the checklists below (the checklists are not exhaustive).

In relation to endpoint security measures (ie security software that is distributed to PSDs), the OVPC has indicated that, to ensure an organisation takes reasonable steps to protect data security as required by IPP 4 of the *Information Privacy Act* 2000 *(Vic)* (equivalent to APP 11 of the *Privacy Act 1988* (Cth)), endpoint security products should have the following capabilities (OVPC, *Portable Storage Devices: Privacy Survey* (2011) at 32):

- to whitelist or blacklist PSDs;
- to provide detailed logs of PSD access, including details of data that has been transferred to and from the PSD, and the user that initiated the transfer;
- to control the type of access permitted to specific users or PSDs (eg read or write access, types of files, amount of data transferred and times that the device can be used); and
- to enforce encryption on device connection.

Work-issued devices

Issue	Guidance
Risk assessment	Regular risk assessments of each type of PSD should be conducted to determine risk levels as the nature, functions and capabilities of devices changes.
Types of devices	Types of PSDs that are permitted should be reviewed. Certain devices may be prohibited because, for example, their utility is outweighed by their risks or because the devices are new and their risks are not yet fully known or understood.
Software controls	Appropriate software controls should be installed on PSDs to provide endpoint protection (see above at [205.75]).
Limitation of data storage	Restrictions should be placed on what data can be stored on PSDs. Generally, such data storage should not be permitted unless absolutely necessary. Data that can be so stored should be restricted to the minimum necessary for the relevant purpose.
Personal use	Consideration should be give to whether, and in what circumstances, work PSDs may be used for personal use.
Data transfers to PSDs	Policy should address what files and data are permitted to be transferred to PSDs. Consideration should be given to whether it is possible and appropriate to use security software to track transfers of files and data to PSDs.

Software applications, websites, web-servers and web-hosts

Related materials
• [153.60] Websites - Data security

[205.80] In relation to the use of software applications, websites, web-servers and web-hosts (being businesses that provide space on a web-server owned or leased for use by clients who use them to host, among other things, their websites, online shopping software applications and databases containing customer information), case notes issued by the Information Commissioner indicate that data security obligations generally require an entity to ensure (see *AAPT and Melbourne IT: Own motion investigation report* [2013] AICmrCN 1, *Telstra Corporation Limited: Own motion investigation report* [2014] AICmrCN 1; *Medvet Science Pty Ltd: Own motion investigation report* [2012] AICmrCN 5; *Multicard: Own motion investigation report* [2014] AICmrCN 2; *Cupid Media Pty Ltd: Own motion investigation report* [2014] AICmrCN 3):

- data on web-servers is appropriately assessed and classified to determine whether it includes personal information and the sensitivity of that information;
- in relation to software applications (particularly those installed on web-servers) –
    - existing and emerging security risks are monitored, identified and addressed (including the application of security patches);
    - vulnerability assessment and scanning and effective lifecycle management occurs;
    - regular reviews of all IT applications held internally or with external providers are conducted to ensure the entity is aware of applications held;
    - security patches are applied when they are issued;
    - new versions are installed when they are released, on the basis that older versions are generally known to have vulnerabilities;
- in regard to third party web-hosts – appropriate contractual measures are taken to ensure the security of information stored on servers, including, where appropriate, specification of who is responsible for each of the above security measures.
- in relation to websites:
    - access to non-public content is restricted to authorised and authenticated users;
    - directory browsing is disabled;
    - the site is configured to ensure search engine robots do not search and index non-public content;
    - databases containing user passwords should store them in encrypted form.

In *AAPT and Melbourne IT*, a server holding the first respondent's ("outsourcer") customer information had been compromised by hackers. The server was hosted by a third party ("web-host"), the second respondent. Data on the server was accessed by the hackers via a software application installed on the server. At the time of the incident, security patches were up to date on the software application. However, the application itself was seven years old. Several newer versions of the application were available, the most recent of which had security features that may have prevented the attack.

A contract between the outsourcer and the web-host stated that the server was to be fully managed and maintained on the outsourcer's behalf, with the exception of custom application content and data, which was to be the outsourcer's responsibility. The web-host described the software application as a "customer managed application" and, in its view, it was the outsourcer's responsibility to update the application when newer versions became available. The web-host took responsibility for keeping

existing applications patched. The contract contained some provisions requiring the web-host to have security arrangements in place for data held on the server. However, the Commissioner found that the contract did not address matters relating to assessment of whether personal information is being held and its sensitivity and monitoring of software security risks.

The Commissioner concluded that the outsourcer breached its data security obligations by failing to take its own steps to appropriately manage and protect the information and not having adequate contractual measures in place to protect the personal information held on the server (the ACMA had also earlier found that the outsourcer had breached cl 6.8.1 of the *Telecommunications Consumer Protections Code C628:2007* by failing to require the web-host to protect the privacy of its customers' information).

The Commissioner recommended that the outsourcer take the following measures:

- identify and address existing or emerging security risks in connection with the software application;
- conduct regular reviews of all IT applications held internally or with external providers to ensure the outsourcer is aware of applications held;
- take steps to ensure all IT applications held internally or externally which hold or use personal information are subject to vulnerability assessment and testing, regular vulnerability scanning and have effective lifecycle management;
- clearly allocate responsibility for lifecycle management of applications;
- conduct regular audits of the outsourcer's IT security framework to ensure that security measures are working effectively, and that policies and procedures relating to data security are being complied with;
- undertake further training for IT staff and relevant business units to increase their understanding of their data security obligations (including lifecycle management of IT applications), data security risks and threats;
- undertake steps to ensure appropriate classification of data it holds, either internally or externally, including whether it includes personal information and the sensitivity of that information;
- review the terms of the contracts it has with IT suppliers that hold or manage the outsourcer data to ensure clarity around which party has responsibility for identifying and addressing data security issues (eg vulnerabilities associated with old versions of IT applications).

Data security breaches and notification

Related materials
- OAIC, *Guide to securing personal information* (2015) at p 36 ("Data breaches")
- Cyber-attacks and hacking (at [7.5410])
- OAIC, *Guide to developing a data breach response plan* (2016)
- OAIC, *Data breach notification: A guide to handling personal information security breaches* (2012)
- OVPC, *Responding to Privacy Breaches* (2008)
- OVPC, *Responding to Privacy Breaches – Checklist* (2008)
- OICQ, *Privacy breach management and notification*

Managing data security incidents

[205.85] In the event that an entity suffers a data security breach, it is essential that it responds promptly and appropriately to manage the incident. Breaches may occur as a result of, for example:

- loss or theft of laptops, portable storage devices or hardcopy records;
- inadequate access controls for customer information stored on websites;
- emailing documents to incorrect recipients;
- mailing-list errors resulting in letters being sent to incorrect recipients;

- hacking;
- non-secure disposal of computer hardware or hardcopy records;
- employees accessing personal information for non-work related purposes.

Entities should have in place incident management policies and procedures, in particular:

- reporting of events – formal event reporting procedures should be in place to ensure incidents and weaknesses in information systems are communicated to specific designated personnel to enable an immediate response, for example, via pager or email that is monitored after hours to persons who are designated to be available on a 24/7 basis to respond to breach alerts;
- incident response plan – procedures should be in place to handle incidents once they have been reported to ensure they are appropriately managed. The federal Commissioner has published guidelines on developing an incident response plan, including on what the plan should cover, who should form part of a response team and actions that should be taken (containment, evaluation of risks, notification and prevention of future incidents) – see OAIC, *Guide to developing a data breach response plan* (2016).

Data breach notification

Related materials
[21.20] Investigations by Commissioner - Commissioner's approach

[205.87] Currently, there is no requirement under the Privacy Act to notify the Information Commissioner of a data security breach. The Information Commissioner's *Data breach notification: A guide to handling personal information security breaches* (2012) provides voluntary guidelines on how to respond to data security breaches involving unauthorised exposure of personal information, including when to notify affected individuals and data protection authorities (the Queensland Information Commissioner has also issued guidelines – see the "Related materials" box above). The guidelines include four key steps to consider when responding to a breach:

- Step 1: Contain the breach and do a preliminary assessment
- Step 2: Evaluate the risks associated with the breach
- Step 3: Consider notification (to affected individuals and authorities)
- Step 4: Prevent future breaches

Notification will not always be an appropriate response. A key factor to consider will be the risk level associated with the breach. If there is a high risk of serious harm to affected individuals, they should be notified. On the other hand, providing notification about low risk breaches may cause affected individuals undue anxiety and, if the practice of notification becomes widespread for such breaches, de-sensitise individuals to notices from other entities.

In regard to notifying the OAIC, the Commissioner's guidelines state the following factors should be considered:

- any applicable legislation that may require notification
- the type of the personal information involved and whether there is a real risk of serious harm arising from the breach, including non-monetary losses
- whether a large number of people were affected by the breach
- whether the information was fully recovered without further disclosure
- whether the affected individuals have been notified, and
- if there is a reasonable expectation that the OAIC may receive complaints or inquiries about the breach.

In regard to how the OAIC will respond if notified, the OAIC has stated (OAIC, "Woolworths data breach – finalisation of enquiries" (media release, 21 July 2015)):

> In approaching data breaches that are notified to the OAIC by the affected organisation, the OAIC initially makes enquiries to confirm that the organisation involved is appropriately handling the breach to protect the

personal information of affected individuals and prevent a recurrence. Depending on the response from the organisation, the OAIC will then determine what further action, if any, it needs to take in relation to the matter.

Where the incident affects large numbers of individuals, notification to the OAIC will assist it in responding to enquiries and complaints regarding the incident by affected individuals. The OAIC will, for example, be familiar with the circumstances of the breach and steps the entity has taken to address the matter.

Where an entity elects *not* to notify the Commissioner of a breach, it should make a detailed file note of the considerations it took into account in making this decision (which should include those outlined in the Commissioner's guidelines) and the reasons which led to that conclusion. In the event that the Commissioner subsequently investigates the incident, this will enable the entity to provide evidence that it gave serious consideration to voluntarily reporting the incident, a factor that the Commissioner will likely take into account in determining whether the entity responded appropriately in managing the breach.

In December 2015, the federal Government released an exposure draft of the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*. The draft Bill seeks to introduce a new "Part IIIC – Notification of serious data breaches" into the Privacy Act which, if passed, will establish a mandatory data breach notification scheme.

Overseas experience shows that, in the event of a breach, the costs associated with complying with mandatory notification schemes are high, providing entities with a strong incentive to invest in data security measures to avoid breaches and the subsequent application of notification obligations. The Government's *Draft Early Assessment Regulatory Impact Statement* for the draft bill cites a report that found the average total cost of a data breach under the current voluntary notification scheme is $2.82 million, with a cost of $144 per lost or stolen record (Ponemon Institute, *2015 Cost of Data Breach Study: Australia* at p 1). Overseas studies put the average cost of complying with mandatory notification obligations much higher. Damage to brand reputation is also likely to be high, particularly as information about the breach will necessarily be in the public domain following notification and, at least for high profile entities, likely be reported in the media.

Under the proposed scheme, entities will be required to notify the Commissioner and affected individuals if a "serious data breach" occurs. A "serious data breach" will generally occur if there is unauthorised access to, or disclosure of, personal information that results in a real risk of "serious harm" to any of the individuals to whom the information relates. Such a breach could occur, for example, following malicious access to stored information (eg a hacker attack) or an accidental loss (eg of IT equipment or hard copy documents). "Harm" is defined to include physical, psychological, emotional, reputational, economic and financial harm.

Other key elements of the proposed scheme include:

- An entity notifying affected individuals will be required to take reasonable steps to notify them of its identity and contact details, a description of the breach, the kinds of information concerned and recommendations about the steps they should take in response to the breach. Entities could notify individuals by whatever channels they normally use (eg email, post, phone). The Government's *Discussion paper: Mandatory data breach notification* (2015) confirms that the "reasonable steps" test means that "[s]ometimes it might be reasonable for an entity to take no steps to notify each affected individual – for example, if it was not possible to identify each individual, if the entity did not hold contact details for each individual, or if the cost of notifying each individual would be excessive in all of the circumstances".
- If it is not practicable to notify each affected individual, the entity will be required to publish a notice about the breach on the entity's website (if it has one) and take reasonable steps to publicise the notice (eg through a social media post or an advertisement in online or print media).

- Where the information concerned had been disclosed to an overseas third party (eg a service provider) pursuant to APP 8.1 (which requires reasonable steps be taken to ensure the recipient does not breach the APPs – see [7.3600]) and the overseas recipient suffers the breach, the Australian entity will be subject to the notification obligations (consistent with its existing liability for the acts and practices of the overseas recipient under s 16C of the Privacy Act – see [7.3580]).
- Where an entity suspects, but is not certain, that a serious data breach has occurred, the entity will have a 30 day period in which to investigate and assess this.
- An entity that fails to become aware of a serious data breach that it reasonably should have detected will not be compliant with its notification obligations.
- The Commissioner will be able to direct an entity to undertake notification if notification has not occurred after a serious data breach.
- Entities will be able to apply to the Commissioner for an exemption from notification, which can be granted only if notification would be contrary to the public interest.

The proposed provisions would apply in relation to information about one or more individuals. Accordingly, the breach will not have to be a large scale one for the obligations to take effect. In contrast, under the Commissioner's current voluntary data breach notification guidelines, whether a large number of people are affected by the breach is stated to be a relevant consideration (but not determinative in itself) in relation to whether notification should be made.

Failure to comply with notification obligations would fall under the Privacy Act's existing enforcement and civil penalties framework.

Cases studies – incident response measures

[205.90] Case studies of incident response measures taken by entities in response to data security breaches, and whether the Commissioner considered the responses adequate, are set out below.

- The respondent, a global software company, suffered a cyber-attack resulting in an illegal copy of a backup database being made available on the internet. The database contained customer information (usernames, email addresses, encrypted passwords, plain text password hints, names, addresses, phone numbers and encrypted credit card details), including that of over 1.7 million Australian users. The respondent took the following measures which were considered by the Commissioner to be appropriate:
    - disconnected the compromised database server from its network;
    - initiated an investigation into the breach;
    - blacklisted relevant IP addresses;
    - changed passwords for all administrator accounts;
    - reset passwords for affected users;
    - notified affected individuals;
    - notified the banks processing its customer payments so that they could work with payment card companies and card-issuing banks to help protect customers' accounts;
    - notified law enforcement authorities;
    - sent takedown requests to third party site operators that had published the compromised personal information;
    - implemented steps to mitigate against future data breaches;
    - engaged an auditor to confirm its remediation steps: *Adobe Systems Software Ireland: Own motion investigation report* [2015] AICmrCN 1.
- In June 2015, Woolworths unintentionally emailed eVoucher details to 400 customers. Woolworths advised the OAIC that the cause was a fault in an automated system. The OAIC contacted Woolworths about the incident after the incident was reported in the media.