Update 6 | Issued: 30 March 2015

About this bulletin

This bulletin reproduces key sections of new content inserted into the *Australian Privacy Law Handbook* in the most recent update to the service to enable subscribers to keep up-to-date with developments by reviewing new commentary and case summaries. The content is incorporated under relevant headings to show topics to which it relates.

CONTENTS

Annotated Australian Privacy Principles

[7.100] APP 1—open and transparent management of personal information

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

In July 2014, the Victorian Privacy Commissioner formally adopted *Privacy by Design* (PbD), a standard developed by the Information and Privacy Commissioner of Ontario in the 1990s (available at <www.privacybydesign.ca>), as a core policy to underpin information privacy management in the Victorian public sector. PbD 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.

In October 2014, the Victorian Commissioner also published *Privacy by Design: Effective Privacy Management in the Victorian public sector*, 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 to assist in ensuring privacy is built-in to new systems and processes.

Content of privacy policy

[7.280] A non-exhaustive list of information that must be contained in a privacy policy is set out in APP 1.4. Notes in regard to various elements are set out below:

- ...
- paras (f), (g) – these paragraphs require notification of disclosures to "overseas recipients". An entity "can be regarded as likely to disclose personal information to an overseas recipient if it is the entity's current practice or it has established plans to do so" (*APPG* at [1.28]). An "overseas recipient" has the meaning specified in APP 8.1 (s 6(1)), which generally defines it as a third party (ie not the entity or individual to whom the information relates) who is not in Australia. Accordingly, this includes a disclosure to a related body corporate. The definition does not make any reference to where the personal information is located (ie in Australia or overseas). Accordingly, a disclosure to an overseas recipient will, in addition to including a transfer of information to a person overseas, also encompass circumstances where information that is stored in Australia (eg on an Australian network) is accessed by someone overseas. Routing information, in transit, through a server located outside Australia, as well as making information available to an overseas office of the entity, would usually be considered a "use" and not a disclosure (and therefore does not need to be covered by the notification): see *APPG* at [1.29]. An example of when it may be impracticable to specify the countries of overseas recipients is where information is likely to be disclosed to numerous recipients and the burden of determining where they are likely to be located is "excessively time-consuming, costly or inconvenient in all the circumstances". However, the fact that it is merely inconvenient, time-consuming or imposes some cost is not sufficient (*APPG* at [1.30]). If information is disclosed to numerous overseas locations, a list of countries may be included in an appendix to the policy or, for online policies, in a separate regularly updated list to which a link is provided. Where it is not practicable to specify the countries, the entity could instead identify general regions (eg European Union countries) (*APPG* at [1.31]).

Providing copy of privacy policy (APP 1.6)

[7.300] An entity can decline to provide a copy of its privacy policy in a particular form if it would not be reasonable in the circumstances to meet the request. The steps that are reasonable will depend upon (*APPG* at [1.40]):

- other steps taken to make it available;

- practicability (eg excessive time and cost involved) – however, the fact that it is \inconvenient, time-consuming or imposes some cost is not sufficient in itself to warrant refusing to provide a copy of the policy);
- sensitivity of the information (the more sensitive it is, the more rigorous the steps required);
- any unique or unusual information handling practices involved;
- any reasons given for the request;
- any special needs (eg disability) of the requester.

A privacy policy should usually be made available free of charge. However, if a charge is imposed in special circumstances, the reason for the charge and the basis of calculation should be clearly communicated and explained before the policy is made available in the requested form, and the charge should be calculated at the lowest reasonable cost (*APPG* at [1.41]). If a request for access in a particular form is declined, the entity should provide an explanation for the decision. The entity should be prepared to undertake reasonable consultation with the requester about the request (*APPG* at [1.42]).

[7.540] APP 2—anonymity and pseudonymity

Application of right of pseudonymity

[7.600] Transacting pseudonymously usually involves the individual concerned providing the entity with a name, term or other descriptor that does not identify them and through which he or she can be addressed specifically, such as an email address that does not contain their name or an online user name (*APPG* at [2.6]).

The use of a pseudonym does not necessarily mean that an individual cannot be identified. The individual may subsequently choose to divulge their identity, or provide identifying information (eg credit card details). An entity may have in place a registration system that enables a person to participate by pseudonym (eg in a moderated online discussion forum) on condition that the person is identifiable to the forum moderator or the entity (*APPG* at [2.7]).

Personal information should only be linked to a pseudonym if this is required or authorised by law, it is impracticable for the entity to act differently, or the individual has consented to providing or linking the additional information (*APPG* at [2.8]).

Exceptions – "impracticable" to deal with unidentified individuals (APP 2.2(b))

[7.640] In special circumstances, it may be "impracticable" where the burden of the inconvenience, time and cost of dealing with an unidentified or pseudonymous individual, or of changing an existing system or practice to include the option of anonymous or pseudonymous dealings, would be excessive in all the circumstances. However, this is more likely to be a transitional rather than an ongoing justification. Entities are generally expected to design and maintain information collection systems that incorporate anonymous and pseudonymous options (*APPG* at [2.21]).

Providing "the option" of dealing anonymously or pseudonymously

[7.660] It is implicit in APP 2 that an entity should ensure that, if applicable, individuals are made aware of their opportunity to deal anonymously or by pseudonym with the entity. If anonymity or pseudonymity is the default setting, this does not apply (*APPG* at [2.12]).

The steps an entity should take will depend on the nature of the relevant dealing. For example, an entity's privacy policy could explain the circumstances in which an individual may deal anonymously or pseudonymously, and the procedures for doing so. The policy could go further and explain how the entity manages pseudonyms and any linked personal information, and any consequences for dealing anonymously or pseudonymously (*APPG* at [2.13]). Other options include notification via (*APPG* at [2.14]):

- prominent notices on relevant webpages or indicating relevant fields in online forms are not mandatory;
- automated call answering messages;
- verbal notification.

[7.998] APP 3—collection of solicited personal information

Missing persons (s 16A table, item 3)

[7.1222] The *Privacy (Persons Reported as Missing) Rule 2014*, made under s 16A(2) of the Act, applies for the purposes of item 3 of the table in s 16A(1). The rule outlines requirements regarding the collection, use and disclosure of personal information pursuant to the exemption.

Collection by "lawful" and "fair" means

Cases

C was blind and used a sighted guide. C had undergone surgery for a medical condition and was required to wear a medical device. C travelled on a flight and obtained a letter from his treating hospital for the purpose of ensuring C was fit to travel. However, the letter did not contain all information required. C presented the letter at the airport check-in and travelled without incident. On his return flight, C was subjected to a series of questions by the respondent about his medical condition in the airport departure lounge to ensure he was fit to fly. This was done in the presence of his sighted guide (who did not know the details of his medical condition) and other passengers. C was required to state his name, date of birth, medical condition and where physical manifestations of his condition were located. *Outcome:* The collection was conducted in an unreasonably intrusive way in breach of NPP 1.2 (similar to APP 3.5). Although there may have been an obligation on C to provide the information requested to determine fitness to travel, such obligation did not warrant collection in such an unreasonably intrusive way. Even if a private room was not available, the questioning should have been conducted in an area away from other people. The respondent was required, pursuant to a s 52 determination, to make a written apology, review its staff training in the handling of sensitive information and pay $8,500 compensation for non-economic (distress and humiliation): *'BO' and AeroCare Pty Ltd* [2014] AICmr 32.

[7.1500] APP 4—dealing with unsolicited personal information

Meaning of unsolicited information

[7.1560] APP 4 deals solely with information that is not solicited. "Unsolicited" personal information is personal information that an entity receives but has taken no active steps to collect (*APPG* at [4.7]).

Examples of unsolicited information may include (*APPG* at [4.7]):

- misdirected mail received;
- correspondence to ministers from members of the community;
- a petition sent to an entity that contains names and addresses;
- a CV sent on an individual's own initiative and not in response to a job advertisement;
- a promotional flyer containing personal information.

Generally, where an entity requests personal information but receives additional personal information that it has not requested (eg an individual attaches to an application form financial records that were not requested), the additional information should be treated as unsolicited information (*APPG* at [4.8]).

"Lawful" and "reasonable" to destroy or de-identify unsolicited information (APP 4.3)

[7.1580] APP 4.3 only requires personal information to be destroyed or de-identified "if it is lawful and reasonable to do so".

It is lawful for an entity to destroy or de-identify unsolicited personal information if it is not unlawful to do so: that is, if the destruction or de-identification is not criminal, illegal or prohibited or proscribed by law. Unlawful activity does not include breach of a contract (*APPG* at [4.21]).

For relevant considerations when determining whether it is reasonable to destroy or de-identify information, see *APPG* at [4.25].

[7.2000] APP 5—notification of the collection of personal information

Steps that are "reasonable in the circumstances" to provide notice at or before collection

Cases

[7.2061] ***Collection from individual concerned.*** C was blind and used a sighted guide. C had undergone surgery for a medical condition and was required to wear a medical device. C travelled on a flight and obtained a letter from his treating hospital for the purpose of ensuring C was fit to travel. However, the letter did not contain all information required. C presented the letter at the airport check-in and travelled without incident. On his return flight, C was subjected to a series of questions by the respondent organisation about his medical condition in the airport departure lounge to ensure he was fit to fly. The respondent did not provide a privacy collection notice or inform C of its identity or the purpose of the collection of his personal information. *Outcome:* The respondent breached NPP 1.3 (equivalent to APP 5) by failing to ensure C was aware of its identity and to explain the purpose of collection. The respondent could not assume C understood why his information was being collected: *'BO' and AeroCare Pty Ltd* [2014] AICmr 32.

C was a judge of the Federal Circuit Court in the family law jurisdiction and regularly received threats from parties whose matters he had heard. Safety measures provided for by the Court to protect judges and their families included setting up alarm systems at their homes and suppressing their contact details on publicly accessible databases. C contacted Telstra to have a phone line connected to his home as part of an alarm system installed by the Court. C informed Telstra that the sole purpose of the line was for the alarm system and not for any other purpose. Telstra did not inform C that it would publish C's information in the White Pages and its privacy collection notice referred only to disclosures to "the manager of the Integrated Public Number Database, and other organisations as required or authorised by law'" but not to disclosures through the White Pages. Telstra set up the line and published C's name, address and phone number in the White Pages (hardcopy and online). Conciliation of the matter failed and was determined through a s 52 determination. *Outcome:* Telstra breached NPP 1.3 by failing to take reasonable steps to provide notice to C that it would use and disclose the information for the purpose of publishing it in the White Pages. Telstra could not assume that C knew that his personal information would be published in the White Pages unless he requested a silent line feature. Telstra bore the onus of showing that C was aware that it was Telstra's usual business practice to disclose phone line information. Telstra apologised in writing to C, reviewed its processes to require sales consultants to notify each prospective customer that their phone number would be listed in the White Pages and that they have the option of taking out a silent line, reviewed its Privacy Statement to make specific reference to the collection of personal information for the purpose of publication in the White Pages and paid C $18,000 for non-economic loss: *'DK' and Telstra Corporation Limited* [2014] AICmr 118.

Content of notices

[7.2078] The matters that must be set out in a privacy collection notice are listed in APP 5.2.

...

For the purposes of APP 5.2(f), a "usual" disclosure is "one that occurs regularly, under an agreed arrangement, or that can reasonably be predicted or anticipated. It does not include a disclosure that may occur in exceptional or special circumstances (such as a disclosure under a lawful warrant to a law enforcement agency)" (*APPG* at [5.23]) ... A legal obligation to disclose personal information does not obviate the requirement to state in a collection notice persons to whom personal information would normally be disclosed. Accordingly, reasonable steps must still be taken to provide notice of the disclosure: *'DK' and Telstra Corporation Limited* [2014] AICmr 118 at [35], [64].

For the purposes of APP 5.2(i) and (j), the requirements only apply to "disclosures". Routing personal information, in transit, through servers located outside Australia would usually be considered a "use", rather than a "disclosure". Similarly, making information accessible to an overseas office of the entity is a "use" and not a "disclosure". Accordingly, it is not necessary to include details about these types of uses in the collection notice (*APPG* at [5.29]). It may be

impracticable to specify the countries of overseas recipients where information is likely to be disclosed to numerous overseas recipients and the burden of determining where they are located is excessively time-consuming, inconvenient or costly in the circumstances (although, the fact that it will be time-consuming or inconvenient or that there will be a cost is not in itself sufficient) (*APPG* at [5.30]).

[7.2500] APP 6—use or disclosure of personal information

Cases

Licensing authorities

[7.2523.80] The NSW Roads and Traffic Authority (RTA) was responsible for issuing licence cards to security industry personnel. Legislation required license cards to contain specified details (eg photo of the licensee, signature of licensee and class of licence) and that personnel display the cards in a clearly visible manner. However, license cards contained more information than was required, including licensees' dates of birth. The Commissioner was of the view that the inclusion of dates of birth was without legislative authority and was an unwarranted intrusion of privacy. The RTA amended its practices to no longer include dates of birth on license cards and offered to issue replacement cards for existing licence-holders: *Privacy Complaint Investigation Report, Excessive personal information on security industry licence cards (NSW Police Force & Roads and Traffic Authority of NSW)* (2012).

[7.2575]

6.2 [use or disclosure within reasonable expectations]

"Reasonably expect"

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.

"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].

[7.2625]

(b) [use or disclosure required or authorised by law]

"Required" vs "authorised" by law

In *'DK' and Telstra Corporation Limited* [2014] AICmr 118, Telstra was required to publish customer's personal information in the White Pages by the terms of its carrier licence, which amounted to use and disclosure for a secondary purpose. The terms of the licence were declared by the Minister pursuant to s 63(3) of the *Telecommunications Act 1997*. The Commissioner held that the direct source of the authorisation to use and disclose the information was the Minister's declaration and not the Act (ie the law). Accordingly, it could not be said that any disclosure made in accordance with the declaration was a disclosure "required or authorised by law". However, as the authorisation was made pursuant to a law, the disclosure was authorised under that law. Telstra was, therefore, authorised under law to publish the information.

Cases

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. The terms of the licence were declared by the Minister pursuant to s 63(3) of the *Telecommunications Act 1997*. *Outcome:* As the authorisation was made pursuant to the Act, the disclosure was authorised under that law. Telstra was, therefore, authorised under law to publish the information under NPP 2.1(g) (equivalent to APP 6.2(b)): *'DK' and Telstra Corporation Limited* [2014] AICmr 118.

[7.3000] APP 7—direct marketing

"Reasonably expect" use or disclosure for direct marketing (APP 7.2(b))

[7.3080] The Commissioner has provided guidance that the "reasonably expect" test "is an objective test that has regard to what a reasonable person, who is properly informed, would expect in the circumstances. This is a question of fact in each individual case. It is the responsibility of the organisation to be able to justify its conduct" (*APPG* at [7.15]). Relevant considerations when assessing this will include whether (*APPG* at [7.16]):

- the individual has consented;
- the individual has been notified in a privacy collection notice that the use or disclosure will occur;
- the organisation has made the individual aware that they can request not to receive direct marketing communications and the individual has not made such a request.

The level of confidentiality or sensitivity of the information will also likely be relevant. If it is high, reasonable expectations as to secondary purposes will be more restricted.

An organisation should not assume an individual would reasonably expect use or disclosure for direct marketing just because it believes the individual would welcome the direct marketing, for example, because of the individual's profession, interest or hobby (*APPG* at [7.17]).

An individual is not likely to have a reasonable expectation of use or disclosure for direct marketing if the organisation has notified the individual that their personal information will only be used for a particular purpose unrelated to direct marketing (eg a privacy collection notice states the information will only be used for processing an application) (*APPG* at [7.18]).

Opt-out notices and facilities (APPs 7.2, 7.3, 7.7)

[7.3100] APPs 7.2 and 7.3 each require the provision of an opt-out facility in relation to all direct marketing communications. APP 7.3 also requires the inclusion of a statement in each direct marketing communication that the individual may opt-out.

An opt-out facility should comprise of (*APPG* at 7.19]):

- a clear and prominent explanation of how to opt-out;
- a process which requires minimal time and effort;

- a straightforward and accessible communication channel, although this does not necessarily have to be the same channel by which the direct marketing communications were sent (eg communications were sent via mail but the opt-out facility is via email);
- a process that is free or involves only nominal cost (eg local phone call, text message or stamp).

An opt-out mechanism can provide the individual with the ability to tailor their preferences for direct marketing communications (eg opt-out of some but not all categories of communications), but should always provide the ability to opt-out of all communications (*APPG* at [7.30]).

Examples of opt-out facilities, according to medium of communication, include (*APPG* at [7.29]):

- email marketing - by replying with "Unsubscribe" in the subject line or providing a link to an unsubscribe facility;
- SMS - by replying with "Stop" in the message;
- telemarketing - verbally informing of the right to opt-out from future calls;
- mail - including instructions on how to opt-out in each communication.

A statement notifying the individual that they may opt-out (under APP 7.3) should meet the following criteria (*APPG* at [7.28]):

- be in plain English;
- be positioned prominently and not hidden amongst other text;
- be published in a font size and type which is easy to read (eg at least the same font size as the main body of text).

APP 7.7(a) requires an organisation to give effect to an opt-out request within a "reasonable period". This would generally be no more than 30 days (*APPG* at [7.37]).

Notifying individuals of information source (APPs 7.6 and 7.7)

[7.3140] APP 7.6 provides a right for individuals to ask an organisation to disclose its source of their personal information. Organisations must comply with such a request, unless it is impracticable or unreasonable to do so. Responses must be provided free of charge and within a reasonable period. The obligation is, however, qualified by a "practical and reasonable" test (APP 7.7(b)). If an organisation concludes that it is impracticable or unreasonable to provide the notification, it must be able to justify this (*APPG* at [7.46]). Relevant considerations in assessing this will include (*APPG* at [7.46]):

- any adverse consequences if notification is not given;
- length of time since the information was collected;
- if the information was collected prior to the commencement of APP 7 - whether the source was recorded;
- any excessive time and cost involved (however, the fact that some time and cost is involved will not in itself be sufficient to warrant refusal to notify).

Notification of the source must be given within a "reasonable period" after the request is made (APP 7.7(b)). This should generally be 30 days unless special circumstances apply (*APPG* at [7.47]).

[7.3500] APP 8—cross-border disclosure of personal information

Reasonable steps to ensure recipient does not breach APPs

[7.3610] What constitutes "reasonable steps" will depend on the circumstances. Generally, an entity will be required to enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the information in accordance with the APPs (other than APP 1) (*APPG* at [8.16]). For commentary on contractual measures that should be taken with contractors, see [138.58].

However, the Commissioner has indicated that whether reasonable steps to ensure the overseas recipient does not breach the APPs requires a contract to be entered into, the terms of the contract, and the steps the APP entity takes to monitor compliance with any contract

(such as auditing), will depend upon the circumstances. Relevant factors will include (*APPG* at [8.17]):

- the sensitivity of the information;
- the entity's relationship with the overseas recipient – more rigorous steps may be required if the entity has not previously disclosed information to the recipient (assumedly on the basis that previous good experience with the entity may support a conclusion that the contractor has robust information management practices);
- the severity of adverse consequences if the recipient mishandles the information;
- existing technical and operational privacy safeguards implemented by the recipient;
- the practicability (including any excessive time and cost) involved.

Where an agency discloses information to a recipient that is engaged as a contracted service provider, the agency must also comply with s 95B which requires the agency to take contractual measures to ensure that the contracted service provider does not do an act, or engage in a practice, that would breach an APP if done by that agency (see [45.30]). Contractual measures taken under s 95B will generally satisfy the requirement in APP 8.1 (*APPG* at [8.18]).

Based on the Commissioner's guidance, whether a general contractual provision of the former type would be sufficient to amount to "reasonable steps" will depend on the circumstances. However, in any case, it is preferable to have terms state specific standards and protections. The Commissioner has previously indicated, in relation to obligations for agencies that existed under s 95B (to take contractual measures to ensure contractors did not engage in an act or practice that breached the former IPPs), that a general contractual term would not be sufficient (see OPC, *Private Sector Information Sheet 14 – Privacy Obligations for Commonwealth Contracts* (2001) at p 4).

Where making an overseas disclosure pursuant to APP 8.1, an entity should also consider obtaining the following from the overseas recipient:

- a warranty that it will not do any act that would breach the APPs if it were bound by them;
- an indemnity in relation to any loss or damage suffered by the Australian entity as a result of any such act by the recipient, or any of its contractors or agents.

For general commentary on the meaning of the phrase "such steps as are reasonable in the circumstances", see [7.25].

Public interest determinations

[7.3649] The following public interest determinations exempt authorised deposit-taking institutions (within the meaning of the *Banking Act 1959*) from compliance with APP 8.1 in relation to the processing of international money transfers: *Privacy (International Money Transfers) Public Interest Determination 2015 (No. 1)*; *Privacy (International Money Transfers) Public Interest Determination 2015 (No. 2)*. The determinations are in force until 25 February 2020.

"Law or binding scheme"

[7.3657] A "law or binding scheme" could, for example, be a privacy statute, a statute that contains provisions imposing data privacy obligations (eg taxation laws), an enforceable industry scheme or privacy code or binding corporate rules (see [90.25]) (APPG at [8.21]). The Government's *Companion Guide – Australian Privacy Principles* (June 2010) provides (at 13) "'binding scheme' is intended to ... include self-regulatory or other international arrangements that provide the necessary level of protection".

An overseas recipient generally will not be subject to a law or binding scheme where, for example, it is exempt from complying with a data privacy law or can opt-out of a binding scheme without notice or returning or destroying the relevant data (*APPG* at [8.22]).

"Substantially similar" privacy protections

[7.3660] A substantially similar law or binding scheme would provide a comparable, or a higher, level of privacy protection to that provided by the APPs. Each provision of the law or scheme is not required to correspond directly to an equivalent APP. Rather, it is the overall effect of the law or scheme that is relevant. Factors that may indicate that the overall effect is

substantially similar include the law or scheme (*APPG* at [8.23]):

- includes a comparable definition of personal information;
- regulates the collection of information in a comparable way;
- requires the recipient to notify individuals about the collection of their information;
- requires the recipient to only use or disclose the information for authorised purposes;
- includes comparable data quality and data security standards;
- includes a right to access and seek correction of information.

Enforcement mechanisms (APP 8.2(a)(ii))

[7.3667] In regard to ensuring an individual has access to an enforcement mechanism in the recipient country, a range of dispute resolution or complaint handling models may satisfy this requirement (eg a regulatory body similar to the OAIC, an accredited dispute resolution scheme, an independent tribunal or a court) (*APPG* at [8.25]). Effective enforcement mechanisms may be expressly provided for under statute or a binding scheme or may take effect through the operation of cross-border enforcement arrangements between the OAIC and a data protection commissioner in the foreign jurisdiction (*Explanatory Memorandum* at pp 83-84.8.25).

An enforcement mechanism should meet two key requirements – it should (*APPG* at [8.25]):

- be accessible to the individual; and
- have effective powers to enforce the privacy or data protections in the law or binding scheme.

Relevant considerations in deciding whether there is an accessible and effective enforcement mechanism include whether the mechanism (*APPG* at [8.25]):

- is independent of the overseas recipient;
- has authority to consider a breach of any of the privacy or data protections in the law or binding scheme;
- is accessible to an individual (eg the existence of the scheme is publicly known and can be accessed directly without any unreasonable charge);
- has the power to make a finding that the overseas recipient is in breach of the law or binding scheme and to provide a remedy;
- is required to operate according to principles of procedural fairness.

The mechanism may be a single mechanism or a combination of mechanisms. It may be established by the law or binding scheme that contains the privacy or data protections, or by another law or binding scheme or, alternatively, may take effect through the operation of cross-border enforcement arrangements between the OAIC and an appropriate regulatory authority in the foreign jurisdiction (*APPG* at [8.26]).

Consent after notification that APP 8.1 will not apply (APP 8.2(b))

[7.3705] The Commissioner has indicated that the statement should, at a minimum, explain that if the individual consents to the disclosure and the overseas recipient handles the personal information in breach of the APPs (*APPG* at [8.28]):

- the entity will not be accountable under the Privacy Act;
- the individual will not be able to seek redress under the Privacy Act.

The Commissioner has indicated that the statement could also explain any other practical effects or risks associated with the disclosure, including (*APPG* at [8.30]):

- the overseas recipient may not be subject to any privacy obligations or to any principles similar to the APPs;
- the individual may not be able to seek redress in the overseas jurisdiction;
- the overseas recipient is subject to a foreign law that could compel the disclosure of personal information to a third party, such as an overseas authority.

Consent is not required before every proposed cross-border disclosure. Consent may be provided for multiple disclosures to the relevant overseas recipient (*APPG* at [8.32]).

[7.4500] APP 10—quality of personal information

"Accurate"

[7.4530] Personal information is inaccurate if it contains an error or defect or if it is misleading. An opinion about an individual is not inaccurate merely because the individual disagrees with the opinion. For APP 10 purposes, an opinion may be "accurate" if it is presented as an opinion and not objective fact, it accurately records the view held by the relevant person and it is an informed assessment that takes into account competing facts and views (*APPG* at [10.12]-[10.14]).

"Complete"

[7.4536] Personal information is "incomplete" if it presents a partial or misleading picture, as opposed to a true and full picture (*APPG* at [10.17]).

Incomplete information can be misleading in various ways; for example, where it:

- omits relevant information – eg a report refers to an individual's conviction, without stating that the conviction was later quashed; or
- contains opinions expressed as fact.

Reasonable steps to ensure quality

[7.4580] Reasonable steps to review the quality of personal information should be taken (at p 85):

- in regard to collection – at the time of collection; and
- in regard to use and disclosure – at the time of the use or disclosure.

What constitutes reasonable steps will depend on the circumstances. Relevant considerations will include (*APPG* at [10.6]):

- the sensitivity 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 quality is not ensured;
- 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.

Other considerations will include likely uses and disclosures and any previous checks conducted.

In some circumstances, it will be reasonable for an entity to take no steps to ensure the quality of information. For example, where an entity collects information from a reliable source (eg the individual concerned) (*APPG* at [10.7]).

Examples of reasonable steps an entity could take include (*APPG* at [10.8]):

- implementing internal practices, procedures and systems to audit, monitor, identify and correct poor quality information;
- implementing protocols that ensure information is collected and recorded in a consistent format;
- ensuring updated or new information is promptly added to relevant records;
- providing individuals with a simple means to review and update their information (eg online);
- prompting individuals to keep their information up-to-date when engaging with them;
- contacting the individual to verify the quality of information when it is used or disclosed, particularly if there has been a lengthy period since collection;
- where information is collected from a third party – ensuring the third party has appropriate collection practices (this could entail contractual measures regarding data quality or undertaking due diligence on the third party's data quality practices);
- where information is used for a secondary purpose – assessing the quality of the information having regard to that purpose.

[7.5000] APP 11—security of personal information

"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]).

Cases (Securing data)

Cyber-attacks and hacking

[7.5410] A server holding the first respondent's ("outsourcer") customer information (identity and billing details) had been compromised by hackers. Security patches were up to date on the software application used to store the information, 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. *Outcome:* 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 outsourcer had also failed to destroy or permanently de-identify information no longer in use (the ACMA had also earlier found that AAPT breached cl 6.8.1 of the *Telecommunications Consumer Protections Code C628:2007* by failing to require its server host, the second respondent, to protect the privacy of its customers' personal information): *AAPT and Melbourne IT: Own motion investigation report* [2013] AICmrCN 1.

Websites

[7.5450] Personal information about thousands of applicants for Maritime Security Identity Cards was made publicly accessible online through the respondent's website. The information included names, photos, dates of birth, addresses and partial credit card details. The respondent had incorrectly configured the website to allow directory browsing and did not configure the site to prevent search engine robots from indexing non-public content. The information was indexed by Google. *Outcome:* The respondent breached its data security obligations by failing to restrict access to authorised and authenticated users, to disable directory browsing and to configure its website to prevent search engine robots from indexing non-public content: *Multicard: Own motion investigation report* [2014] AICmrCN 2.

Files containing personal information about approximately 15,775 of the respondent's customers were publicly accessible online for a period of 14 months. Access controls were accidentally turned off by a service provider engaged to extend access controls to enable authorised partners to access the data, making the source files publicly accessible online. The files were indexed by Google. *Outcome:* The respondent had breached data security obligations by failing to properly configure its website to prevent the unwanted indexation of content by search engine robots such as Googlebot, to appropriately monitor security (demonstrated by the length of the exposure) and to take conduct vulnerability testing: *Telstra Corporation Limited: Own motion investigation report* [2014] AICmrCN 1.

The respondent operated dating websites based on personal profiles. Hackers accessed personal information contained in thousands of user accounts and posted it on one of their own servers. The compromised information included names, dates of birth, email addresses and passwords. Other information contained in users' profiles and held by the respondent included sensitive information, such as racial or ethnic origin, religious beliefs or affiliations and sexual preferences or practices. Security measures surrounding the information included patch application and management, antivirus software protection on all servers and database segregation. However, user passwords were stored in plain text, rather than encrypted, form. *Outcome:* The respondent breached its data security obligations by failing to encrypt passwords. As the respondent handled sensitive information, more stringent security steps were required to secure the information than may be required of an entity that did not handle

sensitive information. Information, patch management and intrusion detection systems were adequate: *Cupid Media Pty Ltd: Own motion investigation report* [2014] AICmrCN 3.

Shipping addresses and order details of around 800 customers who had purchased paternity, drug and alcohol test kits had been stored in the respondent's online web store and captured via a Google cache. *Outcome:* The respondent had failed to meet data security requirements. The accessibility of address information on the internet constituted unlawful disclosure. Reasonable steps had not been taken to protect the personal information. The online ordering software did not include appropriate security. The development and quality management practices associated with the web store application were deficient. Multiple security flaws existed and there was a lack of security testing associated with the product: *Medvet Science Pty Ltd: Own motion investigation report* [2012] AICmrCN 5.

Storage of paper records

[7.5470] The respondent had previously operated a medical centre. After closure of the centre, the respondent continued to store complete paper medical records (including, among other things, around 960 complete patient medical files and staff pay records) in a locked garden shed at the rear of the site for more than two years. The shed was subsequently broken into and the boxes of medical records were compromised. *Outcome:* The respondent had breached its data security obligations. There are no circumstances in which it would be reasonable to store sensitive information in a temporary structure such as a garden shed. The shed was located at a site no longer used by the respondent, which meant access to the shed could not be effectively monitored: *Pound Road Medical Centre: Own motion investigation report* [2014] AICmrCN 4.

Complaint handling

[7.5480] C attended a school managed by the respondent Diocese (both of which were part of the same legal entity) at which he claimed he was sexually abused by a teacher. Several years after the alleged abuse, C lodged a complaint with the Diocese about the abuse sought a settlement. The Diocese's legal advisers wrote to the Diocese in relation to the claim and forwarded a copy of the correspondence, which included details about C's allegations, to the school. At a school council meeting, documents detailing C's allegations were provided to members of the council and one unauthorised non-council staff member who attended the meeting. *Outcome:* The Diocese breached its data security obligations. Firstly, the Diocese failed to redact C's name from the documents. This should have been done in view of: the increased potential for misuse, loss, unauthorised access or disclosure because of the number of people involved in the process; the fact that C's identity was not relevant for the council as it was merely considering the draft correspondence to C and the proposal for settlement (as opposed to investigating the claim) and in view of the period of time since C attended the school; the sensitivity of the information. If C's identity was required, it could have been provided solely at the meeting, rather than in the documents, to limit the risk of disclosure. Awareness by council members of confidentiality obligations alone was not sufficient. Secondly, the Diocese failed to adequately check and control to whom the documents were distributed. The Diocese was required to pay $7,500 for non-economic loss (stress): *'CM' and Corporation of the Synod of the Diocese of Brisbane* [2014] AICmr 86.

Public area

[7.5490] C was blind and used a sighted guide. C had undergone surgery for a medical condition and was required to wear a medical device. C travelled on a flight and obtained a letter from his treating hospital for the purpose of ensuring C was fit to travel. However, the letter did not contain all information required. C presented the letter at the airport check-in and travelled without incident. On his return flight, C was subjected to a series of questions by the respondent about his medical condition in the airport departure lounge to ensure he was fit to fly. This was done in the presence of his sighted guide (who did not know the details of his medical condition) and other passengers. C was required to state his name, date of birth, medical condition and where physical manifestations of his condition were located. *Outcome:* The respondent breached its data security obligations under NPP 4.1 (equivalent to APP 11.1) by failing to take reasonable steps to protect C's information from unreasonable disclosure. The respondent was required, pursuant to a s 52 determination, to make a written apology, review its staff training in the handling of sensitive information and pay $8,500

compensation for non-economic (distress and humiliation): *'BO' and AeroCare Pty Ltd* [2014] AICmr 32.

Reasonable steps to destroy or de-identify information

[7.5607] To comply with this obligation, an entity must develop systems, policies and procedures to identify information the entity no longer needs and a process for how the destruction or de-identification of the information will occur: *AAPT and Melbourne IT: Own motion investigation report* [2013] AICmrCN 1. The need for such processes is particularly acute in the context of electronic records as the low, and often negligible, cost of storing and retaining such information does not drive a need for regular review and destruction, unlike with hardcopy records. In *AAPT and Melbourne IT*, the Commissioner found the first respondent breached its data security obligations by failing to delete electronic records stored online which were no longer in use (see case summary below).

Cases (Data destruction/de-identification)

Digital records

[7.5998.5] The respondent operated dating websites based on personal profiles. Hackers accessed personal information contained in thousands of user accounts and posted it on one of their own servers. A significant number of the compromised user accounts included unused and duplicate accounts. Further, the respondent did not have any processes for identifying such accounts and destroying or de-identifying the personal information contained in them. *Outcome:* The respondent breached its data security obligations by failing to have such processes in place: *Cupid Media Pty Ltd: Own motion investigation report* [2014] AICmrCN 3.

Files containing personal information about approximately 15,775 of the respondent's customers were made publicly accessible online for a period of 14 months after access controls were accidentally turned off by a service provider. Information in the files was between four and seven years old and the respondent advised that it did not have an immediate commercial need for the data. Nothing in the respondent's data retention policy required the source files to be retained on the online platform. *Outcome:* The respondent had breached data security obligations by failing to have in place systems to identify personal information that was not being used or disclosed for a permissible purpose or to destroy or de-identify such information. To assist in preventing future data breaches, the respondent conducted internal reorganisation to support the central management of software and platforms, increased security controls and established a security team tasked with searching for any customer data that may be accessible publicly or through search robots: *Telstra Corporation Limited: Own motion investigation report* [2014] AICmrCN 1.

A server holding the first respondent's ("outsourcer") customer information (identity and billing details) had been compromised by hackers. The compromised servers contained old customer information that was no longer required by the outsourcer. The outsourcer's *Information Management Policy*, *Information Management Guidelines* and *Data Storage for Archive and Back up Standard* outlined data retention periods and systems, however, there was low awareness of these and they were not being followed. *Outcome:* The outsourcer breached its data security obligations by failing to destroy or permanently de-identify information no longer in use. The outsourcer implemented staff training on data retention and destruction: *AAPT and Melbourne IT: Own motion investigation report* [2013] AICmrCN 1.

Medical records

[7.5998.10] The respondent had previously operated a medical centre. After closure of the centre, the respondent continued to store complete paper medical records (including, among other things, around 960 complete patient medical files and staff pay records) in a locked garden shed at the rear of the site for more than two years. The shed was subsequently broken into and the boxes of medical records were compromised. It became apparent that the majority of the records related to patients who had ceased to be active patients at least 11 years earlier. *Outcome:* The respondent had breached its obligation to identify and securely destroy or de-identify personal information that was no longer being used or required, including medical records that were eligible to be destroyed in accordance with the *Health Records Act 2001* (Vic). The respondent responded appropriately to the breach by: reviewing its privacy policy; developing a data breach response plan; conducting privacy training with all

personnel; undertaking a risk assessment regarding its management of personal information; and implementing measures to review paper based patient health records annually to identify whether they may be de-identified or securely destroyed: *Pound Road Medical Centre: Own motion investigation report* [2014] AICmrCN 4.

[7.6000] 12 Australian Privacy Principle 12—access to personal information

Scope and operation

[7.6023] 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 a record being held in storage by a third party). In these circumstances, the entity must grant access and cannot simply refer the individual to the third party that has physical possession. However, the individual has a separate right to request access from the third party if it is bound by the Privacy Act (*APPG* at [12.7]).

An agency that has placed a record of personal information in the care of the National Archives of Australia, or in the custody of the Australian War Memorial, is considered to be the agency that holds the record for the purposes of the Privacy Act (s 10(4)) (*APPG* at [12.8]).

[7.6085]

(b) [unreasonable impact on the privacy of other individuals]

"Unreasonable impact"

[7.6088] Relevant considerations in assessing this will include (*APPG* at [12.38]-[12.39]):

- the sensitivity of the information;
- the reasonable expectations of the other individual about how the information will be handled (eg if they were present when the information was given, access may not have an unreasonable impact);
- the source of the information (eg if the individual requesting access provided the information about the other person, access may not have an unreasonable impact);
- whether the information about the other individual can be redacted from the record;
- whether access could be provided through an intermediary;
- the views of the other individual (they may be consulted if it would not pose an unacceptable privacy risk for the individual requesting access);
- whether the other individual consents.

Other means of access

12.6 ...

Mutually agreed intermediary (APP 12.6)

[7.6370] The role of a mutually agreed intermediary under APP 1.6 is to enable an individual to be given access to their personal information and to have the content of that information explained, where direct access would otherwise be refused (*APPG* at [12.73]). An example of where this might occur is where a health service provider refuses access to a psychological assessment on the grounds it may lead the individual to self-harm, but providing access through an intermediary may not pose the same threat.

In seeking an individual's agreement to use an intermediary, an entity should explain the process and the type of access that will be provided. Depending on the nature of the information, the intermediary may need particular skills or knowledge (eg to be a qualified health service provider where giving access to health information) (*APPG* at [12.74]).

If agreement cannot be reached on whom to use as the intermediary, the entity must still take reasonable steps to give access through another manner that meets the needs of the entity and the individual (*APPG* at [12.75]).

[7.6410]

Refusal to give access

12.9 ...

Contents of notice

[7.6420] The reasons for refusal should explain, as applicable (*APPG* at [12.82]):

- that the entity does not hold the information;
- the ground of refusal;
- that access cannot be given in the manner requested and the reason why;
- that the steps necessary to grant access in a way that meets the needs of the entity and individual are not reasonable in the circumstances.

The notice could also set out steps the individual could take that would enable access to be given (eg narrow the scope of the request) (*APPG* at [12.84]).

An entity is not required to provide its reasons for refusing access to the extent that it would be unreasonable to do so. This may occur where, for example (*APPG* at [12.86]):

- it would prejudice an investigation of unlawful activity;
- for agencies - it would reveal the existence of a document the agency would be entitled to neither confirm nor deny under s 25 of the FOI Act.

The description of the complaint mechanisms should explain the internal and external complaint options and the steps that should be followed. In particular (*APPG* at [12.87]):

- a complaint should first be made in writing to the entity (s 40(1A));
- the entity should be given a reasonable time to respond (usually 30 days);
- any right to take the complaint to an external dispute resolution scheme; and
- that a complaint may be made to the Information Commissioner (s 36).

[7.6500] APP 13—correction of personal information

Interaction with FOI Act (agencies only)

[7.607] For agencies, APP 13 operates alongside the right to amend or annotate personal information in Part V of the *Freedom of Information Act 1982* (FOI Act). There is significant overlap, but also significant differences, between the two sets of procedures, criteria and review mechanisms.

The complaint mechanisms under the Privacy Act and the FOI Act also differ.

It is open to the individual to decide under which Act to lodge a request or complaint. An agency could ensure that people are made aware of both options and the substantive differences, for example, in its privacy policy. More detailed information could be provided in another document, such as a form detailing the procedure for requesting correction (*APPG* at [13.29]).

In regard to Commonwealth records (as defined by the Archives Act), which are likely to include, in almost all cases, all personal information held by agencies, such records can, as a general rule, only be destroyed or altered in accordance with s 24 of the Archives Act. Further, s 26 of that Act makes it an offence to alter a Commonwealth record that is over 15 years old. In relation to such records, and more generally, it may be reasonable (and consistent with statutory requirements) to (*APPG* at [13.48]):

- retain a version of a record which contains incorrect information;
- associate a statement to clarify the inaccuracy and either include the correct information in the note or cross referencing where it is held.

Reasonable steps to correct

[7.6572] What constitutes reasonable steps to correct information will depend on the circumstances. It may, for example, include making deletions or alterations to a record, or declining to correct personal information if it would be unreasonable to take such steps (*APPG* at [13.47]). Relevant considerations will include (*APPG* at [13.47]):

- the sensitivity of the information;
- possible adverse consequences if a correction is not made;
- 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;
- the likelihood the entity will use or disclose the information (eg if it is low and the cost of correction would be high, it may be reasonable to not take any steps to correct);
- the purpose for which the information is held;
- record keeping requirements that apply to the information under law;
- whether the information held by the entity is in the physical possession of a third party (if so, it may be appropriate to require the third party to make the correction).

[7.6600]

Notification of correction to third parties

13.2 ...

Scope and operation

[7.6605] The Commissioner has advised that it is implicit in the requirement under APP 13.2 that an entity should take reasonable steps to inform the individual (either at, or as soon as practicable after the time of correction) that they can make a request to notify relevant third parties about corrections (*APPG* at [13.49]).

Relevant considerations in assessing reasonable steps to give notification to a third party will include (*APPG* at [13.50]):

- the sensitivity of the information;
- possible adverse consequences if notification is not provided;
- the nature or importance of the correction (eg minor typographical error vs incorrect address);
- 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.

In certain circumstances, it may be appropriate to notify some, but not, all third party recipients (*APPG* at [13.51]).

[7.6650]

Refusal to correct information

13.3 ...

Contents of notice

[7.6665] The reasons for refusal should explain, as applicable (*APPG* at [13.54]):

- that the entity does not hold the information;
- that the entity is satisfied that the information is accurate, up-to-date, complete, relevant and not misleading having regard to the purposes for which it is held; or
- that the steps necessary to correct the information are not reasonable in the circumstances.

An entity is not required to provide its reasons for refusing to correct information to the extent that it would be unreasonable to do so. This may occur where, for example:

- it would prejudice an investigation of unlawful activity;
- access to health information is denied by a health service provider on the grounds that providing access would pose a serious threat to the life or health of the patient concerned. It is possible that the health service provider would, when stating the exemption that it has relied on, cause the harm that it intended to avoid by denying access, eg by causing the individual to suffer serious mental anguish about the content of the information. In these circumstances, a health service provider should take all reasonable measures to ensure that the reason is provided in a manner that will cause

as little harm as possible to the individual (eg providing an oral explanation of the reason in a compassionate manner to enable the individual to better understand why access has been denied).

The description of the complaint mechanisms should explain the internal and external complaint options and the steps that should be followed. In particular (*APPG* at [13.57]):

- a complaint should first be made in writing to the entity (s 40(1A));
- the entity should be given a reasonable time to respond (usually 30 days);
- any right to take the complaint to an external dispute resolution scheme; and
- that a complaint may be made to the Information Commissioner (s 36).

The individual should be advised of the right under APP 13.4 to request the entity to associate a statement with the information. An agency could also advise an individual of their parallel right under the FOI Act to apply for a record to be amended or annotated and of the right to have the adverse decision reviewed (*APPG* at [13.58]).

Privacy Act 1988 (Cth)

External dispute resolution schemes

[24.105] The Privacy Act empowers the Commissioner to recognise external dispute resolution (EDR) schemes to handle particular privacy-related complaints (s 35A).

The OAIC has issued *Guidelines for recognising external dispute resolution schemes* which include the matters the Commissioner will take into account in considering whether to recognise an EDR scheme, the steps an EDR scheme should take to apply for recognition and the general conditions for ongoing recognition.

Under the Part IIIA credit reporting provisions of the Act, a credit provider is required to be a member of a recognised EDR scheme to be able to disclose credit information about an individual to a credit reporting body.

A public register of EDR schemes is maintained on the Commissioner's website.

Credit reporting provisions – Overview

Introduction

[27.10] The handling of personal information in relation to consumer credit reporting is regulated under Part IIIA ("Credit reporting") of the Privacy Act. Part IIIA applies to "credit reporting bodies" (eg credit reporting agencies), "credit providers" and "affected information recipients" (eg mortgage insurers, trade insurers, debt assignees), as defined by the Act. Part IIIA is supported by the *Privacy (Credit Reporting) Code 2014* (see [27.1010]).

A "credit provider" is defined broadly under the Act and extends to encompass, in addition to main-stream lenders, businesses that provide goods or services to individuals on seven or more days' credit (see [27.22]). Accordingly, such businesses must comply with Part IIIA provisions (for a detailed summary of obligations, see [27.22]).

Generally, the APPs do not apply to credit reporting information held by a credit reporting body, but do apply to other personal information held by it (s 20A). For credit providers and affected information recipients, the APPs apply either in addition to, or instead of, Part IIIA provisions (s 21A), as indicated in the relevant sections (see OAIC, *Privacy fact sheet 40: Credit providers, the APPs and your credit report* for a table of which provisions apply according to type of activity).

Many Part IIIA provisions reflect requirements under the APPs (with similar wording, concepts, structures and exemptions), with necessary adaptations in the context of credit reporting to meet industry and privacy requirements. Commentary under the Annotated APPs chapter (at [7]) regarding the operation of the APPs is directly relevant to the application of many of the credit reporting provisions. Accordingly, cross-references are provided in this chapter, where appropriate, to commentary under the APPs that is relevant to applying Part IIIA provisions.

[27.20] Generally, Part IIIA regulates credit information by outlining:

- the types of personal information that credit providers can disclose to a credit reporting body for the purpose of that information being included in an individual's credit report;
- what entities can handle that information; and
- the purposes for which that information may be handled.

In summary, the following types of personal information can be included in an individual's consumer credit report:

- full name;
- date of birth;
- sex;
- current (or last known) address and previous two addresses;
- name of current (or last known) employer;
- driver's licence number;
- names of credit providers that have provided consumer credit and whether they are licenced by ASIC;
- type of consumer credit provided by the credit providers;
- date on which the consumer credit was made available and terminated;
- limit on the consumer credit;
- certain terms and conditions of that consumer credit, including limited details about repayment and interest obligations;
- repayment history information (eg whether consumer credit payments have been made on time and whether payments have been missed);
- that a credit provider has requested access to information held in a consumer credit report in connection with an application made to it for consumer or commercial credit;
- type and amount of consumer or commercial credit sought in the application;
- a default on a consumer credit payment of $150 or more (ie payment is overdue by 60 days or more);
- a statement that an amount that was recorded as being defaulted upon has since been paid;
- the fact that, as a result of a default, there has been an agreement to vary the terms and conditions of consumer credit or that new consumer credit was provided;
- court judgements that relate to credit provided;
- certain information from the National Personal Insolvency Index, including information that relates to bankruptcy and debt agreements;
- certain publicly available information that relates to activities in Australia and creditworthiness;
- the opinion of a credit provider that a serious credit infringement has been committed;
- credit score (created by the credit reporting body).

A detailed overview of Part IIIA provisions is provided below.

Credit reporting bodies

[27.21] In relation to credit reporting bodies, Part IIIA:

- **Proactive compliance:** requires proactive compliance systems (equivalent to APP 1.2 requirements – for practical commentary on relevant compliance issues, see under [7.100]) (s 20B(2));
- **Privacy policy:** requires a privacy policy about how credit reporting information is managed (equivalent to APP 1.3-1.6 requirements – for practical commentary on relevant compliance issues, including sample privacy policies, see under [7.240] and at [117.10]) (s 20B(3)-(6));
- **Solicited collections:** restricts what information may be collected and requires collection by lawful and fair means (for commentary on what constitutes "lawful and fair" means, see [7.1320]) (s 20C);

- **Unsolicited collections:** regulates how unsolicited credit information must be handled (similar to APP 4 requirements – for practical commentary on relevant compliance issues, see [7.1500]) (s 20D);
- **Permitted uses:** regulates the purposes for which credit reporting information may be used (for practical commentary on relevant compliance issues, see under APP 6 at [7.2500]) (ss 20E, 20K);
- **Permitted disclosures:** regulates the purposes for which, and to whom, credit reporting information may be disclosed (for practical commentary on relevant compliance issues, see under APP 6 at [7.2500]) (ss 20E, 20F, 20K);
- **Direct marketing:** prohibits the use or disclosure of credit reporting information for the purposes of direct marketing, other than in limited circumstances relating to use for pre-screening by a credit provider to assess whether an individual is eligible to receive direct marketing communications (s 20G-J) (for general commentary relating to direct marketing, see under APP 7 at [7.3000]);
- **Government related identifiers:** prohibits the adoption of government related identifiers (equivalent to APP 9.1 – for practical commentary on relevant compliance issues, see under [7.4000]) (s 20L);
- **De-identified credit reporting information:** generally prohibits the use or disclosure of de-identified credit reporting information (however, the use or disclosure of such information by credit reporting bodies is permitted when conducting credit related research that complies with the *Privacy (Credit Related Research) Rule 2014* made under s 20M(3)) (s 20M);
- **Data quality:** requires credit reporting information to be accurate (similar to requirements under APP 10 – for practical commentary on relevant compliance issues, see [7.4500]) (ss 20N, 20P);
- **Data security:** requires credit reporting information to be secure (similar to APP 11 requirements – for practical commentary on relevant compliance issues, see [7.500]) (s 20Q);
- **Access:** provides individuals with a right of access to their credit reporting information, subject to specified exemptions (similar to APP 12 requirements – for practical commentary on relevant compliance issues, see [7.6000]) (s 20R);
- **Correction:** provides individuals with a right to correct their credit reporting information, subject to specified exemptions (similar to APP 13 requirements – for practical commentary on relevant compliance issues, see [7.6500]) (ss 20S-20U);
- **Data destruction/de-identification:** requires destruction or de-identification of credit reporting information after retention periods end (similar to APP 11.2 requirements – for practical commentary on relevant compliance issues, see [7.5600]) (s 20V; see also ss 20Z, 20ZA);
- **Retention periods:** specifies retention periods for credit information (ss 20W, 20X);
- **Destruction in cases of fraud:** requires destruction of credit reporting information in cases where an individual has been a victim of fraud (including identity fraud) and the consumer credit was provided as a result of that fraud (s 20Y).

Credit providers

[27.22] A "credit provider" is defined broadly under s 6G of the Privacy Act. In addition to main-stream lenders, the term also encompasses businesses that provide goods or services to individuals for personal, family or household purposes on terms that allow payment to be deferred for at least seven days. In particular, in addition to banks (and other authorised deposit-taking institutions), and subject to various exceptions, a credit provider includes, among others, an organisation or small business operator:

- for which a substantial part of its business is the provision of credit (s 6G(1)(b));
- in the retail sector that issues credit cards to individuals in connection with its goods or services (s 6G(1)(c));
- that provides credit in connection with its goods or services for which repayment (in part or full) is deferred for at least 7 days (s 6G(2)); or

- that provides credit in connection with the hiring, leasing or renting of its goods where the credit is in force for at least 7 days and no amount, or an amount less than the value of the goods, is paid as a deposit for the return of the goods (but is a credit provider only in relation to the credit) (s 6G(3)).

Accordingly, such organisations and businesses must comply with Part IIIA provisions which include, for example, obligations to have a credit reporting policy (in addition to a privacy policy) (under s 21B) and, if it discloses credit information to a credit reporting body, to be a member of a recognised external dispute resolution scheme (under s 21D), subject to exemptions (see below).

A summary of provisions affecting credit providers is set out below. In relation to credit providers, Part IIIA:

- **Proactive compliance:** requires proactive compliance systems (equivalent to APP 1.2 requirements – for practical commentary on relevant compliance issues, see under [7.100]) (s 21B(2));
- **Privacy policy:** requires a privacy policy about how credit information and credit eligibility information is managed (similar to APP 1.3-1.6 requirements – for practical commentary on relevant compliance issues, including sample privacy policies, see under [7.240] and at [117.10]) (s 21B(3)-(6));
- **Privacy collection notices:** imposes notification requirements in regard to privacy collection notices which apply in addition to requirements for such notices under APP 5 (for practical commentary on relevant compliance issues, including sample privacy collection notices, see under [7.2000] and at [123]) (s 21C) –
    - the Credit Reporting Code provides that these requirements can be met by publishing the relevant details on the credit provider's website (see cl 4.2 of the Code);
- **Disclosures to credit reporting bodies:** imposes requirements regarding when credit information may be disclosed to a credit reporting body (ss 21D, 21F) –
    - this includes obligations to be a member of a recognised external dispute resolution scheme (subject to exemptions set out in the *Privacy Amendment (External Dispute Resolution Scheme-Transitional) Regulation 2014*, including for commercial credit providers) (s 21D(2)) and to provide individuals with 14 days' written notice of an intention to disclose payment default information to a credit reporting body (s 21D(4));
- **Notification of payment in relation to default:** requires notification to a credit reporting body when an amount in relation to which a default has been reported is subsequently paid (s 21E);
- **Permitted uses:** regulates the purposes for which credit eligibility information may be used (ss 21G, 21H);
- **Permitted disclosures:** regulates the purposes for which, and to whom, credit eligibility information may be disclosed (eg with consent, to guarantors, to mortgage insurers, to debt collectors) (ss 21G, 21J-21NA);
- **Notification following refusal of credit:** imposes notification requirements when an application for consumer credit is refused (s 21P);
- **Data quality:** requires credit eligibility information to be accurate (similar to requirements under APP 10 – for practical commentary on relevant compliance issues, see [7.4500]) (ss 21Q, 21R);
- **Data security:** requires credit eligibility information to be secure (similar to APP 11 requirements – for practical commentary on relevant compliance issues, see [7.500]) (s 21S);
- **Access:** provides individuals with a right of access to their credit eligibility information, subject to specified exemptions (similar to APP 12 requirements – for practical commentary on relevant compliance issues, see [7.6000]) (s 21T);
- **Correction:** provides individuals with a right to correct their credit eligibility information, subject to specified exemptions (similar to APP 13 requirements – for practical commentary on relevant compliance issues, see [7.6500]) (ss 21U-21W).

Affected information recipients

[27.23] In relation to affected information recipients, Part IIIA:

- **Proactive compliance:** requires proactive compliance systems (equivalent to APP 1.2 requirements – for practical commentary on relevant compliance issues, see under [7.100]) (s 22A(2));
- **Privacy policy:** requires a privacy policy about how regulated information is managed (equivalent to APP 1.3-1.6 requirements – for practical commentary on relevant compliance issues, including sample privacy policies, see under [7.240] and at [117.10]) (s 22A(3)-(6));
- **Privacy collection notices:** imposes notification requirements in regard to privacy collection notices which apply in addition to requirements for such notices under APP 5 (for practical commentary on relevant compliance issues, including sample privacy collection notices, see under [7.2000] and at [123]) (s 22B);
- **Permitted uses and disclosures:** regulates the purposes for which certain information may be used, and the purposes for which, and to whom, such information may be disclosed by mortgage insurers and trade insurers (s 22C), related bodies corporate (s 22D), credit managers (s 22E) and advisers (s 22F).

Key new resources published by OAIC

- *Guide to securing personal information* (2015)
- *Privacy regulatory action policy* (2014)
- *Guide to privacy regulatory action – exposure draft* (2014)
- *Guide to developing an APP privacy policy* (2014)
- *Guide to undertaking privacy impact assessments* (2014)
- *Privacy business resource 4: De-identification of data and information* (2014)
- *Information policy agency resource 1: De-identification of data and information* (2014)
- *Privacy regulatory action policy* (2014)
- *Guide to privacy regulatory action – exposure draft* (2014)
- *Guidelines on Data Matching in Australian Government Administration* (2014)
- *Mobile privacy: A better practice guide for mobile app developers* (2014)
- *Privacy (Persons Reported as Missing) Rule 2014*

Other privacy laws

New public sector privacy legislation (ACT and VIC)

- The *Information Privacy Act 2014* (ACT) commenced on 1 September 2014. The Act regulates the ACT public sector and replaces the operation of the Privacy Act which, until that date, regulated this sector. The Act contains 11 Territory Privacy Principles (TPPs) which reflect the Commonwealth APPs. The TPPs contain two "marker" principles (ie headings with no content), being TPPs 7 and 9 (regarding direct marketing and Government identifiers respectively and which generally only apply to private sector organisations), to maintain consistency with the numbering of the APPs.
- The *Privacy and Data Protection Act 2014* (Vic) commenced on 17 September 2014. The Act repealed the *Information Privacy Act 2000* (Vic) and the *Commissioner for Law Enforcement Data Security Act 2005* (Vic). The new Act merged the roles of the Privacy Commissioner and the Commissioner for Law Enforcement Data Security to create a single Commissioner for Privacy and Data Protection. The Act re-enacted unchanged the Information Privacy Principles that existed under the Information Privacy Act.

Privacy law reforms – ALRC inquiry into serious invasions of privacy in the digital era

[52.167] The ALRC's final report, entitled *Serious Invasions of Privacy in the Digital Era* (June 2014), contained 16 recommendations. Among other things, the ALRC recommended that, if a statutory cause of action for serious invasion of privacy is to be enacted, it should be a Commonwealth Act and:

- provide that the plaintiff must prove that his or her privacy was invaded in one of the following ways –
  - intrusion upon seclusion, such as by physically intruding into the plaintiff's private space or by watching, listening to or recording the plaintiff's private activities or private affairs; or
  - misuse of private information, such as by collecting or disclosing private information about the plaintiff;
- provide that "private information" includes untrue information, but only if the information would be private if it were true;
- be actionable only where a person in the position of the plaintiff would have had a reasonable expectation of privacy, in all of the circumstances;
- be confined to intentional or reckless invasions of privacy (and should not extend to negligent invasions of privacy) and should not attract strict liability;
- provide that, for the plaintiff to have a cause of action, the court must be satisfied that the public interest in privacy outweighs any countervailing public interest (avoiding the need for a separate public interest defence), including freedom of expression and freedom of the media;
- be subject to specified defences, including necessity, required or authorised by law and consent; and
- provide that courts may award damages, including damages for emotional distress and exemplary damages.

The report also recommended that, if a statutory cause of action for serious invasion of privacy is not enacted, relevant legislation should be amended to provide that, in an action for breach of confidence that concerns a serious invasion of privacy by the misuse, publication or disclosure of private information, the court may award compensation for the plaintiff's emotional distress.

Practical issues and privacy solutions

Consent

Capacity to consent

[126.40] Consent must be given whilst the individual has capacity to understand and communicate. The Commissioner has provided the following guidance (*APPG* at [B.46]):

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

Issues that could affect capacity to consent include age, physical or mental disability, temporary incapacity (eg due to psychotic episode, temporary psychiatric illness or unconsciousness, severe distress or dementia) or limited understanding of English (*APPG* at [B.47]).

If an individual does not have capacity to consent, and this cannot be addressed by providing appropriate support (eg alternative communication method or interpreter) to enable them to have capacity, an entity should consider who can act on the individual's behalf, such

as a guardian, someone with a power of attorney or someone nominated in writing by the individual when they had capacity (*APPG* at [B.48]).

The Commissioner has indicated that if an individual lacks capacity to give consent and another person has authority to act on his or her behalf (such as a guardian or person with an enduring power of attorney), the individual should still be involved as far as is practical in decisions involving their privacy rights (*APPG* at [B.49]).

Opt-in and opt-out consents

[126.47] In regard to opt-out mechanisms to obtain consent, the Commissioner has expressed the view that "[u]se of an opt-out mechanism to infer an individual's consent will only be appropriate in limited circumstances, as the individual's intention in failing to opt-out may be ambiguous" (*APPG* at [B.34]). The Commissioner has indicated that an entity will be in a strong position to show that consent via an opt-out mechanism the more that the following factors, where relevant, are met (*APPG* at [B.34]):

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

Bundled consents

[126.85] Privacy statutes do not prohibit bundled consents and, as such, they are generally permitted, however, the federal Privacy Commissioner has expressed the view that bundled consents have the potential to undermine the voluntary nature of the consent and that, if a bundled consent is contemplated, an entity could, in relation to the proposed collections, uses or disclosures, consider whether (*APPG* at [B.40]):

- it is practicable and reasonable to give the individual the opportunity to refuse consent to one or more of them;
- the individual will be sufficiently informed about each of them;
- the individual will be advised of any consequences of failing to consent to one or more of them.

Disclosures to contractor: notification and transborder data flows

[138.30]

...

Often, a contract will prohibit a contractor from transferring personal information overseas, particularly in the context of government contracts. In July 2014, the Department of Defence's medical and allied health provider to Australian Defence Force personnel, Medibank Health Solutions, terminated its multi-million dollar contract with its optometry service provider, Luxottica Retail Australia Ltd, on the grounds that Luxottica breached its contractual obligations by transferring optical claims information overseas for processing. The case highlights the sensitivity of, and risks associated with, the transfer of personal data overseas by contractors.