Response to Questions on Notice

1. General Issues

Definition of consent

Q1. The Law Institute of Victoria (submission 36, p. 5) has recommended further development of the definition of consent to ensure that it precludes consent from being obtained unreasonably or in a way that undermines the objectives or purposes of the APPs. What is the department's view?

Under recommendation 19-1, the ALRC recommended that the Office of the Privacy Commissioner should develop and publish further guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act*. The ALRC recommended that this guidance should address the factors to be taken into account by agencies and organisations in assessing whether consent has been obtained, cover express and implied consent as it applies in various contexts, and include advice on when it is and is not appropriate to use the mechanism of 'bundled consent'.

In its report, the ALRC rejected the view that the Privacy Act should set out in detail what is required to obtain the requisite consent in the many contexts in which it may be sought. The ALRC also raised doubts about amending the definition of consent in the Privacy Act to include the elements of consent. The ALRC noted that that a statutory definition 'is unable to capture nuances in the evolution of the common law', 'may have unintended consequences' and 'may be interpreted too restrictively'[1].

The Government accepted the key thrust of this recommendation and stated that it would encourage the development and publication of appropriate guidance by the Office of the Australian Information Commissioner (AIC), noting that the decision to provide guidance is a matter for the AIC.

While it is ultimately a matter for the AIC, we anticipate that the guidelines will address matters such as those raised by the Law Council of Victoria.

Q2 Qantas has recommended that APP 3(2) include provision for the situation where consent to the collection of sensitive information can be reasonably inferred from the circumstances of the collection. What is the department's response to this recommendation?

As noted in the answer to question 1, these are matters that we anticipate will be considered by the AIC in developing future guidelines on the meaning of 'consent'.

Under section 15 of the exposure draft, 'consent' means 'express consent or implied consent'. The Department notes that the Privacy Commissioner has previously stated that implied consent 'arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the organisation'[2].

[1] See para 19.62 of ALRC Report, *For Your Information: Australian Privacy Law and Practice*
[2] See *Guidelines to the National Privacy Principles* (2001) at page 22

Q3 Privacy Victoria and others (submission 5, 26, 29, 36) raised concerns about the 'consent exception' under APP 8(2)(b), and suggested that if this provision is retained, it should incorporate a requirement that any such consent be freely express and fully informed, to ensure that any such consent is not implied. What is the department's view?

As noted in the answer to question one, the ALRC raised doubts about amending the definition of 'consent' in the Privacy Act to include the elements of consent. It noted that a statutory definition 'is unable to capture nuances in the evolution of the common law', 'may have unintended consequences' and 'may be interpreted too restrictively'[3].

We anticipate that the matters raised by Privacy Victoria will be considered by the AIC in developing future guidelines on the meaning of consent. The Department notes that the Privacy Commissioner's *Guidelines to the National Privacy Principles* (2001) refers to 'consent' meaning 'voluntary agreement to some act, practice or purpose ... [which] has two elements: knowledge of the matter agreed to, and voluntary agreement' (at page 22).

Q4 Google (submission 16) argued that entities are subject not only to Australian regulation but also foreign regulation, and therefore the reference to 'Australian law' in APP 11(2)(c) and APP 12(3)(g) should be amended to include foreign laws. How do the proposed APPs impact on entities which must comply with foreign laws as well as Australian laws? What is your response to Google's concerns?

The Government's position is that an entity with an Australian link must comply with the APPs relating to an act done, or practice engaged in, within Australia. The existing policy achieved by subsection 6A(4) and section 13D of the Privacy Act will be retained to ensure that an act or practice that is done or engaged in outside Australia will not be an interference with privacy if it is required by an applicable law of a foreign country. For example, an organisation would not breach the APPs if a foreign court judgment required disclosure of personal information in that jurisdiction to assist in investigating a criminal offence.

Q5 Could you please respond to submitters' comments that more personal information will fall within the scope of the proposed legislation by way of the amended definition of personal information? What additional information will be caught under the new definition?

The aspect of the definition that the individual be 'reasonably identifiable' ensures that the definition continues to be based on factors which are relevant to the context and circumstances in which the information is collected and held. Generally, this would mean that the information must be able to be linked to other information that can identify the individual. The 'reasonable' test limits possible identification based on the context and circumstances. While it may be technically possible for an entity to identify a person by the information it holds, it may be that it is not practically possible (for example due to logistics, legislation or contractual restrictions). The test requires consideration of all the means that are reasonably open for an information holder to identify an individual.

The inclusion of a 'reasonably identifiable' element within the definition of 'personal information' does mean that additional informational could fall within the new definition. Some information on its own would not meet the current definition which requires an

[3] See para 19.62 of ALRC Report, *For Your Information: Australian Privacy Law and Practice*

individual's identity to be apparent or reasonably ascertainable, from the information (eg an IP address). However, that information would fall within the new definition if, in conjunction with other information, it could be used to identify an individual. On that basis, it is arguable that additional information would be subject to the privacy protections in the APPs.

Nevertheless, as noted in the Companion Guide, the proposed definition of 'personal information' does not significantly change the scope of the existing concept in the existing Privacy Act. The key conceptual difference revolves around the concepts of 'identity' as used in the current definition, and 'identification' as referred to in the draft definition. The ALRC considered that 'identification' was more consistent with international language and international jurisprudence, and that explanatory material based on the terms 'identified' and 'identifiable' will be more directly relevant.

While the context and circumstances will determine whether particular information falls within the proposed definition, the ALRC used examples of how the new definition could work in practice.

> "6.61 Information that simply allows an individual to be contacted—such as a telephone number, a street address or an IP address in isolation—would not fall within the recommended definition of 'personal information'. As noted above, the *Privacy Act* is not intended to implement an unqualified 'right to be let alone'. As information accretes around a point of contact and it becomes possible to link that information to a particular individual and to target that individual—for example, with advertising material—the information becomes 'personal information' for the purposes of the Act. If an agency or organisation can reasonably identify direct mail recipients by linking data in an address database with particular names in the same or another database, that information is 'personal information' and should be treated as such."

Q6 Further guidance on the meaning of 'personal information' is provided in the Companion Guide. Why is this not included in the definition within the Act?

The Government decided to follow the ALRC's recommendation on this point and include guidance about the definition of 'personal information' in AIC guidelines rather than the Act. The ALRC commented that, 'elements of the definition of 'personal information' will continue to give rise to theoretical uncertainty' and that ongoing practical guidance was necessary from the Privacy Commissioner to indicate how the definition would operate in specific contexts. The Government agreed that the issuing of such guidance would play an important role in assisting organisations, agencies and individuals to understand the application of the new definition, especially given the contextual nature of the definition.

Q7 The Government did not accept the ALRC's recommendations in relation to the privacy of deceased individuals (recommendations 8-1, 8-2, 8-3). The Government response noted that there were 'significant constitutional limitations on the Commonwealth's power to legislate in this area'. Could you provide the committee with an indication of these constitutional limitations?

The Government received advice raising doubts about whether the International Covenant on Civil and Political Rights, on which the Commonwealth was relying, extended to the privacy of deceased persons.

Q8 The South Australian Guardian for Children and Young People (submission 4, p. 3) has raised concerns about inconsistencies between the exposure draft and South Australian information sharing guidelines for the safety of children and their families. Has the department consulted with the Guardian about these concerns? If so what was the outcome?

The main concern giving rise to these comments is the current *Privacy Act* requirement that information only be disclosed where there is a serious and imminent threat to the life and health of an individual. This has caused practical problems in areas such as those canvassed by the South Australian body and currently the only solution lies in a public interest determination being sought from the AIC to allow disclosures that would otherwise breach the Act particularly where the organisation concerned is subject to the IPPs ie where it falls within the definition of a contracted service provider under the Act, or if not a CSP falls within the definition of an organisation for the purposes of the NPPs. The Exposure Draft Bill (APP 6 (2)(c)(i)) removes the necessity of showing imminence which should help address the concerns.

In addition, in the Government response, it was stated that the first stage response will create a platform from which the Government can pursue national harmonisation through discussion with the states and territories. When the first stage response is further developed, the interaction with, and possible inconsistencies between, Commonwealth and State/Territory regimes will be considered.

Q9 The Guardian has asserted that NGOs who receive both Commonwealth and state funding, will be bound by conflicting privacy and information sharing policies. Is this correct, and if so, has the department considered the impact on child safety?

Yes, the Department agrees with the *South Australian Guardian for Children and Young People* (the Guardian) that, under the existing regime, there may be conflicting privacy and information sharing policies and that the proposed regime will need to carefully consider the best way to create a harmonised system that reduces areas of conflict and overlap.

As a point of clarification, we understand the Guardian to be referring to the existing regime (its submission uses the word ‘are contractually bound’, not ‘will be bound’ (para 3.3)). It notes in para 3.1 that the existing Privacy Act applies a test of imminence to disclosure, whereas the South Australian Government’s *Information Sharing Guidelines for Promoting the Safety and Wellbeing of Children, Young People and their Families* (ISG) has a pro-disclosure requirement (ie when risk is serious and anticipated) and does not require that risk be imminent for disclosure to be justified.

After noting the ALRC and Government response advocating the removal of the 'imminence requirement, the Guardian goes on to state that because there is 'strong concordance between the ISG and the proposed APP 6 (use or disclosure of personal information without an imminence element), South Australian NGOs should have 'added confidence to implement the ISG and meet all contractual obligations with regard to protecting privacy'. The Guardian notes that legal advice on the proposed amendment says NGOs implementing the ISG would be protected by proposed APP 6.

The issue of those subject to both Commonwealth and State privacy regimes will be the subject of discussions between the Commonwealth and States/Territories about harmonisation. All parties to those discussions will need to carefully consider what changes are necessary to their respective privacy and information-sharing regimes to ensure an effective harmonised system can be implemented.

Q10 The South Australian Guardian for Children and Young People (submission 4, p. 4) has raised significant concerns about the lack of a 'pro-disclosure' approach to sharing information for the protection of public safety and prevention of harm, abuse and neglect. Could you respond to the Guardian's concerns?

The APPs have been drafted to provide appropriate limits on the use and disclosure of personal information by agencies and organisations. There are a range of legitimate exceptions permitting the use and disclosure of personal information, where an affected individual has not provided consent.

These include where the entity reasonably believes that the use or disclosure of the information is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety, and where it is unreasonable or impracticable to obtain the affected individual's consent to the use or disclosure (APP 6). The Government response noted that, in assessing whether it is 'reasonable or practicable' to seek consent, agencies and organisations could also take into account the potential consequences and nature of the serious threat.

These provisions enable the use and disclosure of personal information where it is necessary for the protection of public safety and the prevention of harm, abuse and neglect. The Department will consider the Senate Committee's recommendations on this issue in advising the Government on possible options for further 'pro-disclosure' measures.

2. AUSTRALIAN PRIVACY PRINCIPLES

Australian Privacy Principle 1 - open and transparent management of personal information

Q11 Why is the more complex term 'such steps as are reasonable in the circumstances' used throughout the APPs rather than 'reasonable steps' which submitters, including OPC, argued was simpler and more familiar to entities?

The Department's view is that the use of the expression 'such steps as are reasonable in the circumstances' ensures that the specific circumstances of each case have to be considered when determining the reasonableness of the steps in question (eg in protecting information, or

ensuring an overseas entity does not breach an APP). While it is arguable that it is implicit in the expression 'reasonable steps' that the surrounding circumstances must be considered, the changed reasonableness formulation makes this explicit. This Department believes this additional clarity and focus on the circumstances surrounding an entity's specific privacy obligation, will have the overall effect of promoting greater compliance with privacy obligations which will be to the benefit of individuals.

Q12 The Law Council of Australia has argued that it is not possible for an entity to put into place practices, procedures and systems to ensure compliance with the APPs and that the words 'will ensure' in APP 1(2)(a) should be replaced with 'have the primary purpose of promoting'. Would you comment on the Council's view?

In including the 'will ensure' formulation, the Government has gone further than the ALRC Report recommendation in requiring agencies and organisations not only to create and maintain a privacy policy but to also demonstrate that they have taken reasonable steps to comply with both the privacy principles and their own privacy policy.

The expressions 'will ensure' and the 'primary purpose of promoting' are different requirements. Under the 'will ensure' formulation in APP 1(2)(a), there is a clear requirement for entities to have practices, procedures and systems that will ensure compliance with the APPs. Replacing it with a 'having the primary purpose of promoting' is a lesser obligation and is not consistent with the Government's approach of promoting high standards of compliance that will require entities to consider how the principles apply to their own circumstances and what steps it should take to implement appropriate policies and practices.

It was the Government's intention for the compliance standards on agencies and organisations to be sufficiently high to enhance privacy protections. The 'will ensure' obligation was included so that privacy protections are built into the design of an entity's system and not 'bolted on' afterwards.

Q13 The requirement that a privacy policy must be in a form 'as is appropriate' was seen as being weak and inferior to that recommended by the Australian Law Reform Commission which required that access must be provided 'electronically'. Why was the ALRC's recommendation not taken up?

The ALRC Report at paragraph 24.71 states that agencies and organisations should take reasonable steps to make their Privacy Policy available electronically (ie. on their website) and that the posting of Privacy Policies on websites is an ideal mechanism for making them generally available. The CyberSpace Law and Policy Centre at the UNSW Faculty of Law also suggested in its submission that there be a requirement that Privacy Policies be available electronically.

The Department believes that an absolute requirement to provide the privacy policy 'electronically' would be a significant burden on organisations without a website or means to otherwise produce an electronic copy. Australian Privacy Principle 1(5)(b) puts agencies and organisations under an obligation to provide an appropriate copy of their privacy policy in a way which is reasonable in all the circumstances, having regard to the agencies or organisations functions, types of business and restrictions. It also addresses issues around

accessibility – eg clients of some entities may not be able to electronically access their policies (eg because they do not have computers) so there should be the option available of providing the policy in any other appropriate format.

Q14 APP 1(6) applies only to individuals. It has been suggested (submission 25) that this is undesirable as requests may come from organisations and the media. Does APP 1(6) accommodate requests from organisations, the media etc?

This provision is based on ALRC Recommendation 24-2, which also uses the terminology 'individual'. There is no definition for 'individual' in either the APPs or the ALRC Report but paragraph 22(1)(aa) of the *Acts Interpretations Act* defines an 'individual' as a 'natural person'.

There is nothing preventing an individual within an organisation or the media from making the request. Therefore, in practice, there should be no foreseeable problem in media or organisations gaining access to relevant documents containing the Privacy Policies of an agency or organisation.

It is not the Government's intention to prevent organisations from making requests for an entity's privacy policy. Therefore, the Department will consider the Senate Committee's recommendations on this issue, including suggestions for improving clarity on this issue.

Australian Privacy Principle 2 – anonymity and pseudonymity

Q15 Yahoo!7 has pointed to the need to ensure that users of online services are identifiable to the services provider even though they may be able to interact with others using screen names. Does APP 2 adequately address the problem outlined by Yahoo?

In its submission, Yahoo!7 noted that it had products and services which require registration so that these details could be relied upon by law enforcement agencies if an alleged crime involving one of its services was to be investigated. Yahoo!7 also believes that companies operating e-commerce websites have a clear need for users to authenticate their identity through the use of credit cards to pay for sales. Yahoo!7 also believes context needs to dictate the appropriateness of allowing users to engage anonymously or to interact pseudonymously within their services.

The Department believes the use of pseudonyms is sufficient to (a) distinguish one individual from another or (b) maintain a transaction history about a person, without retaining a record of their identity. This could be used for agencies or organisations that need this information but do not need to necessarily identify an individual. In developing a framework for the protection of personal information, a key element is whether an agency or organisation needs to collect any personal information (at all) about an individual in order to undertake its functions or interact with the individual. The standard by which agencies or organisations can determine whether personal information is needed should be based on whether it is lawful and practical to interact on an anonymous or pseudonymous basis.

Therefore, if it is unlawful or impracticable for a service provider (such as Yahoo!7) to deal with individuals with anonymity or pseudonymity they would fall under the exception in APP 2(2)(a) and (b). In the cases identified by Yahoo!7 as requiring the collection of

identification information (ie ecommerce websites authenticating identification for credit card purposes; assisting law enforcement agencies to investigate a crime; registering users for particular core services so that the terms of use of the service can be enforced), the Department's view is that these are likely to come within the exception.

Q16 The Office of the Privacy Commissioner has raised concerns that the wording of APP 2(2) could be used by entities to not provide the option to interact anonymously or pseudonymously in all instances not just those where it is 'required or authorised'. Is the department confident that the wording of the exemption in APP 2 ensures that it applies only to those matters where identification is required or authorised by law?

The proposed provision creates the right for an individual to have the option of not identifying themselves, or of using a pseudonym, when dealing with an entity. Under the exception in APP 2(2), that right does not apply if an entity is required or authorised by or under an Australian law, or an order of a court or tribunal, to deal with individuals who have identified themselves. The 'required or authorised' by law exception, has been added into every APP. Although the ALRC report doesn't recommend its inclusion relating to the option to interact anonymously or pseudonymously, it is part of the broader policy of clarifying the operation of that exception.

The OPC has raised concerns that an entity falling within the exception in APP 2(2) could rely on the lawfulness of requiring identification in one instance (eg providing credit card information for e-commerce purposes) to require the individual to identify themselves when dealing with the entity in another instance. The Department notes that there is nothing expressly included in the provision to broaden the scope of the exception in that way.

The ALRC examined the existing 'required or authorised by or under law' exceptions in the Privacy Act (see Chapter 16 generally) and noted generally the need for clarity about the meaning of that expression. As a result, the ALRC recommended that the OPC should develop and publish guidance to clarify when an act or practice will be required or authorised by or under law. Although it is a matter for the AIC, the Department believes that the issue raised by the OPC could be included in those guidelines.

Q17 It was put to the committee that APP 2 does not take into account the Healthcare Identifiers Act 2010 (Epworth Health Care, submission 9, p. 2). How will APP 2 apply in the health sector?

The submission from Epworth HealthCare raises concerns that the right under APP 2 to request a pseudonym when dealing with an entity may be impracticable for hospitals and health care organisations. Epworth HealthCare notes that, while it is possible to deal with patients under pseudonym, individuals are first required to identify themselves, either by Medicare card or with a unique healthcare identifier in order to receive treatment in Australian hospitals. We understand, however, that this is not correct. The system of healthcare identifiers will not alter the way in which anonymous healthcare services are provided. Where it is lawful and practical, individuals can seek treatment and services on an anonymous basis. In these circumstances a healthcare identifier would not be used by the healthcare service.

In general, it is intended that the APPs (including APP 2) will apply to health information and private health service providers in a similar way to the existing regime.

Specific privacy protections for information relating to health services and research will be drafted and referred to the Senate Committee in the next part of the reforms. Therefore, the interaction between those upcoming provisions, the APPs and other generic health legislation and proposed reforms will be further considered at that time.

Australian Privacy Principle 3—collection of solicited personal information

Q18 Does the wording of APP 3(1) need to be tighter to ensure that the aim of privacy protection is achieved?

The wording in APP 3(1) is intended to strike the appropriate balance between the need to protect against the unnecessary collection of personal information and the need for organisations and agencies to collect personal information reasonably necessary for, or directly related to, one or more of the their functions or activities.

The first key element is the inclusion of a 'reasonably necessary' test in relation to the collection of 'personal information other than sensitive information'. This is consistent with the views of the ALRC that an objective test should continue to apply as is currently the case for organisations under NPP 1 (although the ALRC believed that an objective test was implied even with the use of only 'necessary'). The requirement on entities to collect only personal information that is *reasonably* necessary to their functions, requires the collection of personal information to be justifiable on objective grounds, rather than on the subjective views of the entity itself. This will limit inappropriate collection by entities.

The alternative limb of APP 3(1) authorises collection where it is 'directly related to' one or more of the entity's functions or activities. That ensures that there must be a clear connection between the collection and the entity's functions or activities. That aspect of the test appears in the existing IPPs, which bind agencies.

Q19 It has been suggested that the 'directly related to' element is not necessary as it does not improve the effectiveness of the APP – could you respond?

As noted above, the wording 'directly related to' appears in the existing IPPs for agencies. IPP 1.1 states that information must be *collected for a purpose that is lawful [and] directly related to a function or activity*. IPP 1 has operated under the existing regime in circumstances where it may not be possible to meet the 'reasonably necessary' test. This element is being retained because there may be agencies (less so for organisations) that need to collect personal information to effectively carry out defined functions or activities but who may not meet an objective 'reasonably necessary' test.

As noted above, the new APPs are intended to combine the existing IPPs and NPPs, and therefore should be flexible enough to accommodate the requirements of the broader range of entities (ie organisations and agencies) and the different purposes that they have when collecting information.

Q20 OPC has argued that APP 3(2) lowers the existing threshold of NPP 1 and is inconsistent with APP 3(1) as it appears that if an exception in APP 3(3) applies, sensitive information may be collected even if it is not 'reasonably necessary for' or 'directly related to' the entity's functions or activities. Could you respond to this concern?

The Department agrees with the OPC's interpretation that 'sensitive information' could be acquired using an exception in APP 3(3) without the information first needing to be 'reasonably necessary' or 'directly related to' an activity or function of the entity. However, these exceptions are based on circumstances where there is an overriding public interest in collecting the information, for example, to lessen or prevent a serious threat to the life, health or safety of any individual, for public health or safety (APP 3(3)(b)), or for law enforcement purposes (APP 3(3)(c)). Further, there are safeguards built into most of these exceptions to ensure that, even where there are specific special circumstances, there is still a requirement that collection be based on an objective element (either relating to reasonable necessity or reasonable belief of necessity).

Q21 Why was the wording of the emergencies exception (APP 3(3)(b) and APP 6(2)(c)) changed to remove the imminent threat criterion?

The emergencies exception in APP 3(3)(b) relating to the collection of sensitive information, and APP 6(2)(c) relating to use and disclosure of personal information does not include the existing 'serious and imminent' threat formulation in NPP 2.1 (use or disclosure of personal information by an organisation) and IPPs 10 and 11 (use or disclosure of personal information by an agency).

In its report, the ALRC Report stated that the current requirement that a threat must be both serious *and* imminent in these provisions is too difficult to satisfy, sets a 'disproportionately high bar'[4] and can lead to personal information not being used or disclosed in circumstances where there are compelling reasons justifying its use or disclosure.[5] The ALRC further stated that its removal would allow an agency or organisation to take preventative action to stop a threat from developing into a crisis.

The Government accepted the ALRC's view that the imminent threat criterion was too restrictive. However, to address concerns of a number of stakeholders that the removal of this element would inappropriately broaden the exception, a requirement was included that use and disclosure could occur only after consent has first been sought, where to do so is reasonable and practicable. Therefore, both APP 3(3)(b) and APP 6(2)(c) contain additional elements to the exception where 'it is unreasonable or impracticable to obtain the affected individual's consent' to either the collection of sensitive information, or the use or disclosure of personal information.

[4] ALRC Report [para 25.83]
[5] See generally at paras 22.47 – 22.50

Q22 Could the department provide the committee with the reason for including the exemption in relation to missing persons given the ALRC's concerns about possible unintended consequences of such a provision including the endangering of lives?

Under APP 3(3)(g) and APP 6(2)(g), there is an exception to the prohibition against collecting sensitive information and use/disclosure of personal information, where the entity believes it is 'reasonably necessary' to assist any entity, body or person to locate a person who has been reported as missing, and the collection complies with the Australian Privacy Rules made by the Information Commissioner under paragraph 21(a).

The ALRC Report stated at paragraph 25.140 that the creation of an express exception for disclosing personal information to assist in missing person investigations may create adverse consequences in cases where missing persons do not wish to be located. For example, it noted that some missing persons may be choosing to hide from others and trying to disassociate themselves from family or friends. The ALRC believed that creating a general exception in respect of all missing persons risked interfering with the privacy of certain missing individuals and endangering their lives. The ALRC commented that other exceptions would assist in broadening the scope of situations in which disclosure of personal information in missing persons investigations would be authorised, such as the serious threat exception in APP 3(3)(b).

The Government agreed with the ALRC's view that using or disclosing personal information to locate missing persons may often be permitted by other exceptions, but considered that 'an express exception should also apply for those instances where the application of other exceptions is unclear'. For example, some agencies were concerned that the 'serious threat to life' etc exception would not allow them to collect information relating to a missing person who may have gone missing because of health issues. To ensure there are safeguards against improper use of such information, the Government decided that such collection, uses or disclosures should be in accordance with binding rules issued by the AIC, which would be in the form of a legislative instrument and therefore subject to the scrutiny of Parliament.

The Government response included a number of matters that should be included in the rules (outlined in response to Q23 below), and noted that, consistent with the requirement of the *Legislative Instruments Act 2003*, the Privacy Commissioner should consult with relevant stakeholders in making these rules.

Q23 Proposed section 21 allows the Information Commissioner to make rules in relation to the collection of personal information about missing persons provisions. Why will this matter be dealt with by rules rather than in the legislation? What rules do you consider will be made under this provision and will they address the concerns raised in submissions?

These rules will consist of detailed matters relating to the procedures and protocols used by agencies that are more appropriately dealt with in subordinate legislation. It is desirable that these more detailed matters be included in a legislative instrument rather than the Act because this will enable a more flexible response to the wide variety of circumstances in which this issue may arise (eg natural disasters, child abductions).

There is already an existing non-legislative example (Public Interest Determination 7) where the Privacy Commissioner has granted a waiver from compliance with IPP 11.1 which

permits the Department of Foreign Affairs and Trade to disclose personal information of Australians overseas to their next of kin in certain limited circumstances.

Further, under s 17 of the *Legislative Instruments Act 2003*, before a rule-maker makes a legislative instrument, that person must be satisfied that any consultation that is considered by them to be appropriate and that is reasonably practicable to undertake, has been undertaken. As a legislative instrument, the rules will also be subject to Parliamentary disallowance, and so subject to extensive consultation and to Parliamentary scrutiny.

As to what rules could be made under the proposed provision, the matters listed in the Government response (in a non exhaustive list) as appropriate for inclusion in the rules were:

- that uses and disclosures should only be in response to requests from appropriate bodies with recognised authority for investigating reported missing persons;
- that, where reasonable and practicable, the individual's consent should be sought before using or disclosing their personal information;
- where it is either unreasonable or impracticable to obtain consent from the individual, any use or disclosure should not go against any known wishes of the individual;
- disclosure of personal information should be limited to that which is necessary to offer 'proof of life' or contact information; and
- agencies and organisations should take reasonable steps to assess whether disclosure would pose a serious threat to any individual.

Q24 Examples were provided of where organisations may need to collect sensitive personal information from third parties, e.g. to authenticate a customer's identity to satisfy legislative requirements (e.g. anti-money laundering). Why is the exception in APP 3(5)(a) limited to agencies? Will this limitation impact on the ability of organisations to comply with anti-money laundering and counter terrorism legislation?

The exception in APP 3(5)(a) that allows agencies to collect sensitive information from third parties was included because agencies were concerned that they may be in breach of the Act where another law allows or requires them to collect from a number of sources other than the individual, but in the circumstances it would still be practicable and reasonable to go to the individual. An example of this practice is where the Australian Electoral Commission obtains information from Commonwealth agencies and updates the electoral roll using that information.

Organisations are required under the existing NPP 1, where reasonable and practicable, to collect personal information about an individual *only* from that individual. The ALRC did not recommend any change to this.

If an organisation collects information from a third party for identity verification purposes in accordance with legislative requirements under anti-money laundering and counter terrorism legislation, because it had a suspicion that the person is not who they claim to be, it is likely

to be 'unreasonable or impracticable' to collect it from the individual concerned. Therefore, the alternative second element of the exception would apply to allow the collection.

Q25 Could you respond to arguments that APP 3 provides adequate protection for unsolicited personal information? If not, could APP 3 be expanded to include unsolicited information as suggested by the Office of the Privacy Commissioner (submission 39, p. 30) instead of including a separate APP?

The insertion of a separate APP about the collection of unsolicited information is aimed at clarifying the application of the principles explicitly in relation to unsolicited information rather than implicitly as currently occurs with the NPPs. It also confirms that, where an entity could have collected the unsolicited information, it should be treated in accordance with all the privacy principles that apply to the collection of solicited information. To address compliance concerns, APP 4 includes a reasonable period element within which to determine whether or not the entity could have collected the information under APP 3 if the entity had solicited the information, and a 'soon as practicable' test (rather than a requirement to do it immediately) relating to destruction or de-identification.

As to the Office of the Privacy Commissioner's comments about the location of the requirement, it is an important standalone principle of collection that should be included in a separate principle.

Q26 The committee has been provided with examples of where it would be difficult to separate solicited and unsolicited personal information, e.g. provided during a phone call. It was argued that if the unsolicited information could not be separated, then all the information would need to be destroyed. Is this the case?

As we understand, there is a concern that personal information collected through call centres may be a mixture of solicited and unsolicited personal information. For example, in its submission to the Committee, Abacus Australian Mutuals has stated:

> ... if a customer (or another member of that household) discloses extensive personal information that is not required by the Abacus member during a phone call where other *required information* is collected, then a record of the *whole phone call* may need to be destroyed if the not-required information is unable to be separated from the required information (pages 1-2).

A similar view was raised in the submission to the Committee from Westpac, where an example was provided of a customer who had contacted a Westpac call centre, where it is standard practice to record telephone conversations for training and other purposes.[6]

Under the proposed APP 4, the entity must, within a reasonable period after receiving the information, determine whether the unsolicited information could have been collected under APP 3 if the entity had solicited the information. During that process, the entity would be able to determine which information was unsolicited (for example, a recorded phone call may involve being asked standard questions). In addition, the solicited information obtained in these instances would, in practice, be converted into other means such as another form, a

[6] Westpac submission to Committee at page 2

document or on a computer. Therefore, if the entity decided to destroy the electronic recording of the phone discussion, it would still have the solicited information.

Finally, as noted by Westpac, if it is not *reasonable* to do so, the entity is not required to destroy or de-identify the information (APP 4(4)).

The ALRC recognised that there was a need to clarify the meaning of 'unsolicited' personal information. In accepting this recommendation, the Government stated that it encouraged the development and publication of appropriate guidance by the OPC, noting that the decision to provide guidance is a matter for the OPC. While it is ultimately a matter for the AIC, the Department anticipates that the guidelines will address matters such as those raised by the Abacus Australian Mutuals and Westpac.

Q27 It has been put to the committee that APP 4 may preclude the common practice of agencies forwarding incorrectly addressed correspondence, which contains unsolicited personal information, to the appropriate agency. Will this in fact be the case?

The receipt of correspondence by Ministers, members of Parliament and government departments and agencies would, in normal circumstances, be unsolicited. Under APP 4, these entities must, within a reasonable period after receiving the information, determine whether the unsolicited personal information could have been collected under APP 3 if the entity had solicited the information. It is clear that the unsolicited information could have been collected under APP 3 because considering and responding to concerns of members of the public, and referring them to appropriate recipients, are functions of these entities.

Once an entity has determined that the personal information could have been collected under APP 3, it would be possible for the entity to use or disclose the information under APP 6. Under that APP, disclosure to another Minister or government department would be permitted where the individual has consented to the use and disclosure. As the individual has written with queries, views or representations on particular issues, it is within their legitimate expectation that their correspondence will be referred to the appropriate entity within parliament or government.

The recipient entity would also be receiving unsolicited personal information but it also clear that it could have been collected under APP 3 because considering and responding to concerns of members of the public on the particular issues within its responsibilities are directly related to the functions or activities of the entity. The entity may then use the information for the purpose of responding to the correspondence.

Therefore, the practice of agencies forwarding incorrectly addressed correspondence will not be prohibited under the new APPs.

Q28 Professor Greenleaf (submission 25) submitted that the proposed definition of the term 'collects' risks that collection methods which do not involve a third party may be excluded from the requirements under APP 5. Does the department consider the term 'collects' encompasses collection by observation, surveillance or internal generation in the course of transactions?

The submission from Professor Greenleaf and Mr Waters repeated their comments made to the ALRC Inquiry that the definition of 'collects', should expressly include collection by observation, surveillance or internal generation in the course of transactions, to ensure that the notification principle is not read as applying only to collection resulting from 'requests'.

The ALRC found that it was unnecessary to amend the Privacy Act to refer to specific methods of collection because it was clear that personal information could be collected through lawful and fair means (as required by NPP 1) by surveillance, and from publicly available sources, such as books. The ALRC noted that OPC guidance on the requirement for 'fair and lawful' collection recognised that there will be some circumstances, for example, investigation of fraud or other unlawful activity, where covert collection of personal information by surveillance or other means would be fair[7].

As the new draft does not alter the existing position that the *means* of collection of personal information must be 'lawful and fair' (see APP 3(4)), APP 3 or APP 5 do not expressly refer to 'observation, surveillance or internal generation'.

Q29 The Law Institute of Victoria (submission 36) suggested replacing the term 'collects' with 'receives', in APP 5(1) thereby also ensuring that both solicited and unsolicited information are covered by APP 5. Is there a reason that the term 'collects' was used in this provision instead of 'receives'?

The use of the term 'collects' is necessary in APP 5 (notification of collection) to ensure consistency with the operation of, and terminology used in, APP 3 (collecting solicited information) and APP 4 (receiving unsolicited information).

Under APP 4, the first requirement for an entity upon receiving unsolicited personal information is to determine whether the entity could have collected the information under APP 3 if the entity had solicited the information. If the answer to that is yes, APP 5 immediately applies as if the information had been 'collected' as solicited information and the notification requirements under APP 5 must be complied with.

If the entity determines that the entity could not have collected the personal information, the entity must destroy or de-identify the information, as soon as practicable but only if it is lawful and reasonable to do so (APP 4(4)). There is no notification requirement in this instance because the personal information is not being retained for any purpose relating to the identification of the individual.

[7] Para 21.81

Australian Privacy Principle 6 – use or disclosure of personal information

Q30 Various submitters noted concern about the limited application of APP 6(2)(d)(i), and argued that entities should have more discretion regarding disclosures in respect of potential unlawful activity or serious misconduct. However other submitters argued that this provision is not necessary, and could be used to compile and maintain 'blacklists' simply based on suspicion of wrongdoing, with no requirement that any such listed individuals be afforded natural justice. How does the department respond to these comments?

The exception in APP 6(2)(d) is intended to allow entities to use and disclose personal information to assist them in taking appropriate action relating to unlawful activity, or misconduct of a serious nature that relates to the entity's functions or activities.

While the use and disclosure of personal information is permitted for *any* unlawful activity relating to the entity's functions or activities, the use and disclosure of personal information should not be permitted merely for minor breaches of misconduct. These are issues that can be handled internally by the entity without the need to use or disclose an individual's personal information.

Consistent with the ALRC's views, the exception is aimed at internal investigations by an entity about activities within or related to that entity. If an entity believed that there was unlawfulness not related to its own functions and activities, it may be possible to disclose the information under the law enforcement exception in APP 6(2)(e).

Q31 Submitters suggested that the requirement to provide a written note under APP 6(3) should be extended to other exceptions, and that the matters to be included in the written note should be specified. In the department's view would it be beneficial for the sake of clarity, to include such guidance in the exposure draft?

Under APP 6(3), an entity must make a written note of a use or disclosure where it has been permitted under APP 6(2)(e), ie a use or disclosure made because the entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities by, or on behalf of, an enforcement body. Professor Greenleaf and Mr Waters submit that 'this important accountability requirement should extend at least to exceptions (d) (and (f) and (g) if they survive) which are of a similar kind to (e)'. These exceptions relate to unlawful activity/serious misconduct, diplomatic or consular functions or activities, and locating missing persons.

The ALRC found that imposing a general legislative requirement to log use and disclosure is, on balance, untenable[8]. It noted that the sheer volume of use and disclosure of personal information by agencies and organisations on a daily basis would render such a requirement impractical, costly and onerous. However, the ALRC believed there was considerable merit in imposing such a requirement in the special context of law enforcement.

While there is an argument that the unlawful activity exception in APP 6(2)(d) is similar to the law enforcement exception, the ALRC noted that this potential overlap made it seem unnecessary for the Privacy Act to require the logging of all use and disclosure under the unlawful activity exception. The ALRC went on to state:

[8] See paras 25.181 – 25.185

> ... if logging of use and disclosure under the unlawful activity exception were to be mandated, it would create an expectation that logging should be required where personal information is used or disclosed under other, arguably quasi-related, exceptions, such as where use or disclosure is required or authorised by or under law. This would impose potentially disproportionate compliance burdens on agencies and organisations. (para 25.188)

Australian Privacy Principle 7 – direct marketing

Q32 It has been suggested that the complexity of the APPs has been increased with the use of separate provisions for the exceptions relating to the disclosure and use of information for direct marketing. Are you able to advise the committee of the rationale for a separate direct marketing principle?

The rationale for a separate APP dealing with direct marketing derives from ALRC recommendation 26-1, which the Government accepted with amendment. In the Government response, it was stated that a separate principle should be introduced to provide greater clarity regarding the regulation of the use and disclosure of personal information for the purpose of direct marketing.

The ALRC found that, under the existing NPP 2.1 in the Privacy Act, there is 'considerable ambiguity as to whether organisations, which collect personal information that they later intend to use for direct marketing, have collected this information for the secondary purpose of direct marketing'[9]. The ALRC stated that stakeholder concerns regarding the direct marketing activities of some organisations were unlikely to be addressed adequately if the relevant privacy principle only covered secondary purpose direct marketing (as existing existing NPP 2.1 does).

Therefore, the ALRC proposed that the Privacy Act should apply to direct marketing, whether the organisation has collected the individual's personal information for the primary purpose or a secondary purpose of direct marketing. The ALRC noted that the rationale for locating the direct marketing provisions in the general use and disclosure privacy principle would be severely undermined if that proposal was taken up. It was therefore appropriate, given that direct marketing is relevant to other aspects of the information cycle, to create a discrete privacy principle to regulate direct marketing.

Q33 Is the department able to advise the committee why the concept of 'existing and non-existing customers', which was used in the government's initial response to the ALRC report, was not utilised in the exposure draft?

Under ALRC recommendation 26-3, it was stated that organisations should be permitted to use or disclose personal information for the purpose of direct marketing to existing customers over 15 years of age where the:

(a) individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing; and

[9] Para 26.30

(b) organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any direct marketing communications.

The ALRC made another recommendation (26-4) on direct marketing relating to non-existing customers or customers under the age of 15 years. The key recommendation was that use or disclosure for direct marketing should be allowable if consent of the individual is obtained or, in relation to information that was not sensitive information, where it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure.

The Government accepted both recommendations with amendment so that the category of 'sensitive information' should only be used or disclosed for direct marketing to individuals (whether existing customers or not) where it is provided with their consent. The Government response also rejected the need for an age-based distinction to be incorporated into the principle.

As noted in the Companion Guide, the language used in APP 7 is different, but achieves the same policy. Rather than using the term 'existing customer', APP 7 instead focuses on people who have provided information to the entity (ie existing customers) and people who have not provided information (ie non-existing customers). In the case of personal information that is not sensitive information the requirements that are stated in the Government response to apply to 'existing customers' will apply where the information was *collected* from the individual. Further, they apply where the individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing.

The requirements that apply to 'non-existing customers' in the Government response will apply where the information was *not* collected from the individual (or, for logical consistency, where the 'existing customer' would not have reasonably expected that the organisation would use or disclose the information for the purpose of direct marketing).

The drafting approach taken does not divert from the Government's response. The focus in APP 7 is on the key elements of an existing customer relationship, and this is different to the more ambiguous and potentially broader 'existing relationship' concept in the *Spam Act 2003* and the *Do Not Call Register Act 2006*. The approach of distinguishing a customer from a non-existing customer by whether information is provided is the best drafting approach to defining an 'existing customer'. The consequence may be that the requirements in the Privacy Act may differ from sectoral specific legislation but that is necessary to ensure that concepts in the Privacy Act (particularly relating to consent) are consistent and unambiguous.

Q34 The Office of the Privacy Commissioner and ADMA noted that the concept of an 'existing relationship' is used in existing privacy related legislation, guidance on the interpretation of the term exists and it is understood by industry and other stakeholders. Would the adoption of this concept help to maintain consistency and simplicity, and assist understanding of compliance obligations?

The concept of 'existing relationship' is used in the *Spam Act 2003* and the *Do Not Call Register Act 2006* but not in the current Privacy Act. The 'existing relationship' concept

under the Spam Act is explained on the Australian Communications and Media Authority internet site as:

> ***Inferred consent*** relies on a relationship you have with the message sender. The Spam Act provides that consent can be inferred from your conduct or relationship that a message sender has with you. The message sender may decide that because you have an existing relationship, you would be interested in receiving electronic messages about similar products and services. For example, if you subscribe to a magazine or newspaper, it could reasonably be inferred from your ongoing relationship with the publisher that you would be amenable to receiving electronic messages promoting other services the publisher may offer.
>
> In some circumstances, message senders may rely on inferred consent if you have consented to your email address or mobile telephone number being on a marketing database that is sold to businesses.[10]

The first instance described above (subscribing to a magazine) would be covered by APP 7(2) as a direct collection of personal information from an individual. However, the second instance would involve use of personal information by an organisation after it had been collected from another person. In that situation, it is likely that APP 7(3) would apply.

The 'existing relationship' concept in the Spam Act and the Do Not Call Register Act is appropriate for the sectoral specific direct marketing practices relating to electronic messages and phone calls. That concept is included within a broader notion of 'inferred consent', which is based on consent that 'can be reasonably inferred from the conduct, and the business and other relationships, of the individual or organisation concerned'.[11]

However, as noted in previous answers, it is not appropriate to prescribe in detail the elements of consent in the Privacy Act, because providing a statutory definition that applies across a wide variety of contexts remains problematic[12]. The ALRC envisaged that more generally applicable requirements for organisations engaged in the practice of direct marketing would not necessarily be the same as those required for electronic messages and phone calls.

Q35 Some submitters (submissions 2 and 15) recommend aligning APP 7 with the concept of 'inferred consent' which is used in the SPAM and Do Not Call Register Acts. Would this be a better approach to take?

The concept of 'inferred consent' in the Spam Act and the Do Not Call Register Act is not the same as the concept of 'consent' as understood and applied generally throughout the proposed APPs.

In the Privacy Commissioner's Private Sector Information Sheet 26 – *Interaction between the Privacy Act and the Spam Act*, it is stated:

[10] http://www.acma.gov.au/scripts/nc.dll?WEB/STANDARD/1001/pc=PC_310525
[11] *Spam Act 2003* (Cth) sch 2 s 2
[12] ALRC Report at 19.65

> 'While 'express consent' is a common concept to both Acts, 'inferred consent' is not a form of consent used in the Privacy Act ... When compared to how 'implied consent' is applied under the Privacy Act, 'inferred consent' could have a broader meaning. In particular, it permits practices that fall within an individual's reasonable expectations.'

The ALRC did not recommend including a separate concept of consent in the Privacy Act to align general direct marketing rules with sectoral specific direct marketing rules. As noted above, that is necessary to ensure that concepts such as 'consent' in the Privacy Act are consistent and unambiguous.

Q36 Some concerns were raised about how the exposure draft would interact with the SPAM and Do Not Call Register Acts (submissions 7 and 24). Abacus Australian Mutuals (submission 7) noted concerns about the provision under APP 7(6) which appears to indicate that if the SPAM and Do Not Call Register Acts apply, APP 7 will not apply. Are you able to inform the committee about the purpose of this provision?

The Government agreed with the ALRC's recommendation (26-2) that the 'direct marketing' principle should be displaced to the extent that more specific sectoral legislation regulated a particular type of direct marketing or direct marketing by a particular technology.

The ALRC believed this approach was preferable because imposing a blanket rule for all forms of direct marketing was too rigid.[13] It stated that other forms of more intrusive direct marketing should be subject to regulation that differs from the rules applicable to less intrusive forms of direct marketing. It noted that, relying on such sectoral legislation to the exclusion of the *Privacy Act* is problematic, because it leaves loopholes that could encourage other types of direct marketing that also may be intrusive.

This is reflected in APP 7(6) which provides that APP 7 does not apply to the extent that the Spam Act, the Do Not Call Register Act, or any other Act of the Commonwealth prescribed by the regulations applies.

This means that APP 7 will apply to organisations involved in direct marketing relating to electronic messages and phone calls, where acts and practices are not covered by those Acts.

Q37 Clarity has also been sought about how Australian Privacy Principle 7 will interact with the anti-hawking provisions in the Corporations Act, with the Australian Finance Conference suggesting (submission 12) that the provisions of this Act also be included under APP 7(6). Has the department considered this?

The Department's understanding is that, under Chapter 7 of the *Corporations Act 2001*, a person (the 'offeror') must not offer financial products for issue or sale to a retail client in the course of, or because of, an unsolicited meeting or telephone call unless certain conditions are met. An offeror includes issuers and sellers of financial products, as well as their agents and representatives. These prohibitions aim to prevent pressure selling of financial products to retail clients.

[13] ALRC Report at para 26.63

These provisions were not considered as part of the Australian Law Reform Commission inquiry on privacy and therefore not referred to in the Government response. The ALRC may not have made recommendations on this issue because the provisions relate to the consumer protection aspects of unsolicited marketing (hawking) to individuals of specific financial products, rather than relating to the use of personal information in relation to unsolicited marketing, as in the case of the Spam Act and the Do Not Call Register Acts.

Q38 Various submitters commented on the fact that the term 'direct marketing' is not defined in the exposure draft. Is it the department's intention to include a definition of the term? Would this result in more clarity?

No, there is no intention to include a definition of the term 'direct marketing'.

The Privacy Act does not currently define 'direct marketing'. The ALRC's view was that the term should continue to not be defined because there was no consensus about how that term should be defined although its scope is generally understood[14]. In the same paragraph, the ALRC further stated:

> To define direct marketing may unnecessarily confine the application of the 'Direct Marketing' principle. For example, if direct marketing is defined by reference to current practice, but practice later evolves, new methods of direct marketing may not be caught by the definition and so would not be subject to the 'Direct Marketing' principle.

The Government has accepted the view of the ALRC.

Q39 Privacy Law Consulting Australia (submission 24) raised concerns that if the requirements are seen as burdensome, organisations will default to the lowest common denominator in terms of practice. Does the department see this as a concern?

The requirements in APP 7 are intended to allow organisations to undertake legitimate direct marketing activities subject to strict rules aimed at protecting individuals from having their personal information used and disclosed inappropriately. Organisations will be required to consider their existing procedures to ensure that they comply with the new regime.

Obtaining consent and including opt-out facilities should be encouraged as part of a direct marketing organisation's internal procedures. As with other new APPs, there is scope for the AIC to provide guidance on the operation of these provisions. If guidance on the practical workings of APP 7 became necessary, the Department will liaise with the AIC to consider whether to develop guidelines.

Q40 Submitters raised concerns about the lack of a provision to require organisations to provide individuals with the option to opt out of the provision of sensitive information for direct marketing purposes (submissions 24, 25, and 34). Why was such a provision not included?

Under APP 7(1)(a), sensitive information about an individual can only be used for direct marketing by an organisation with the consent of that individual unless the organisation is a

[14] ALRC Report, para 26.32

contracted service provider for a Commonwealth contract and the organisation collected the information for the purpose of meeting an obligation under the contract. The concerns expressed are that, at some point in the future, the individual may want to revoke consent or opt-out (ie no longer wants to receive direct marketing communications from the organisation).

There would be options available to individuals in this instance. First, as noted by the PLCA, consent could be revoked at any time, in which case the organisation could not use sensitive information for direct marketing purposes.

While it is a matter for the AIC, guidelines to be prepared on the meaning of 'consent' are likely to address key issues such as revocation.

In addition, as a result of APP 7(2) and (3), organisations will be required in practice to provide a simple means by which an individual may easily request not to receive direct marketing communications from an organisation. Further, APP 7(4)(a) provides that an individual may request not to receive direct marketing communications from the organisation.

Q41 Privacy Law Consulting Australia (submission 24 p.6) noted that the opt out provisions could be circumvented as APP 7(4)(b) refers to 'direct marketing by other organisations' therefore, if an organisation markets on behalf of persons or bodies which are not organisations as defined by the Act, they will not be required to comply with the provision. What is the department's view on this?

In its submission, the PLCA raised concerns that the reference to 'direct marking by other organisations' in APP 7(4)(b) would refer to an organisation that markets on behalf of persons that are not 'organisations' and who would not need to comply with a request to cease using or disclosing information for that purpose. The PLCA was concerned that the application of this subsection is determined by whether the marketing organisation's *clients* are bound by the Act rather than whether the marketing organisation itself is bound. It believed that it could lead to a direct marketing organisation establishing a separate corporation to market solely for clients that are not "organisations" within the meaning of the Act in order to circumvent the operation of APP 7(4)(b).

The Department does not agree with this interpretation. Under APP 7(4) and (5), an 'organisation' undertaking direct marketing whether on its own, or on behalf of another entity, or facilitating direct marketing by other organisations, is required to respond to a request from an individual under APP 7(4), in accordance with APP 7(5). On the final example, the 'other' organisation undertaking direct marketing will also be subject to the APPs (whether acting on behalf of a small business or not).

Q42 The committee has received evidence (submissions 13 and 15) suggesting that as the requirement to record the source of information cannot be retrospectively applied, the requirement should be limited to non-existing customers. In the department's view, would such a limitation be useful?

The ALRC identified the need to record and disclose to customers the sources of any personal information used or disclosed for the purposes of direct marketing. This

recommendation has been accepted by the Government. In the current draft of the legislation, this policy intent is couched in terms of whether it is reasonable or practicable. Thus, this issue is linked with question 43 below. In many cases, where recent information has been collected about an existing customer, it is reasonable and practicable to expect an organisation to be able to provide an individual with the source of the information. Where that information has been collected at a time where an organisation has not been required to record, and not recorded, the source of this information, it would be impracticable to provide it.

Q43 One submitter (submission 25) noted that under APP 7(5)(c) an organisation does not have to respond to such a request if it is 'impracticable or unreasonable' and argued that this exception is too broad. Is there a risk that organisations will use this provision as an excuse to not provide individuals with details about their own personal information?

This language is consistent with the ALRC recommendation that source disclosure be mandated upon request 'where reasonable and practicable'. While by default such information should be provided to individuals, the ALRC accepted that an organisation may in some cases be unable to provide the information requested. This has been expressed in the legislation as a requirement to provide the information *unless* a test of unreasonableness or impracticability is fulfilled. For example, if the information was recorded at a time where an organisation has not been required to record, and not recorded, the source of this information, then it would be unreasonable to expect an organisation to provide this information.

While some organisations may attempt to misuse this test, it is a necessary element of the legislation to enable the policy goal of source disclosure to existing customers who have not provided information to organisations. It is also possible to clarify this issue in the Explanatory Memorandum when the *Privacy Act* is considered by the Parliament.

Q44 In the department's view, would it be pertinent to include a provision preventing direct marketing to minors?

The Government has noted that the primary purpose of direct marketing provisions in the Privacy Act is to regulate direct marketing via post. Electronic direct marketing, such as that conducted by email or SMS, is regulated by the Spam Act. The Government response noted that there is insufficient evidence that postal direct marketing to young people has resulted in substantial adverse consequences[15].

The ALRC has also recommended that a campaign be developed to inform children and young people about privacy issues. This is a recommendation that will be addressed in the second part of the Government response to the ALRC's review.

[15] See recommendation 26-3

Australian Privacy Principle 8 – cross border disclosure of personal information

Q45 Submission 11 argued that APP 8 is complex and confusing, as it does not explicitly state the intention of the principle, which is explained in the Companion Guide as being that 'if the overseas recipient does an act or practice that would be a breach, then the entity would be liable'. The submitter suggests that the Canadian legislation states the entity's responsibility more clearly, and encourages an organisation to use contractual arrangements to ensure the adequate level of privacy protection is complied with by the third party. Such arrangements were supported by some submitters (submission 11, 15). Has the department considered this approach?

Under APP 8(1), there is a requirement for an entity, before it discloses personal information about an individual to an overseas recipient, to take 'such steps as are reasonable in the circumstances' to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to the information.

In responding to ALRC recommendations 31-2 and 31-3, the Government accepted the general principle that an agency or organisation should remain accountable for personal information that is transferred outside Australia. The Government accepted that there should be a limited number of exceptions to this principle. Further, the Government stated that it was important for the term 'accountable' to be defined so that the scope of the principle is clear to agencies and organisations.

In developing the concept of accountability, a number of different sources were considered, but the key instrument was the APEC Privacy Framework. APEC in turn derived the accountability principle from the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 1980. The OECD Guidelines did not define accountability, relying instead with a statement that 'a data controller should be accountable for complying with measures which give effect to the principles' contained in the Guidelines. APEC Privacy Principle 9 states that:

> A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

The key element of accountability is that an agency or organisation transferring personal information should exercise due diligence and take reasonable steps to ensure the recipient will protect the personal information.

Overseas models such as the Canadian model were examined in the course of developing APP 8. As noted in the submission from Dr Bennett, the Canadian model focuses on the use of 'contractual or other means to provide a comparable level of protection while the information is being processed by a third party'.

One way to meet a requirement that a foreign recipient protect personal information would be to use a contract. However, while contracts will remain useful as important mechanisms for agencies and organisations to impose obligations upon recipients, they should not provide a specific exception on their own from the accountability obligations. As noted in the Companion Guide, it is expected that entities will ordinarily have a contractual relationship with overseas recipients, and that contract would set out the obligations of the overseas recipient. This may not be reasonable in all circumstances but it is the general expectation.

Q46 A number of submitters (submission 13, 14, 15, 19, 25, 28, 41) suggested that the Office of the Privacy Commissioner should compile and publish a list of countries that it considers have privacy legislation equivalent to Australia's to assist entities in complying with their obligations, particularly under APP 8(2)(a) when disclosing information offshore. What is your view on this proposition?

The ALRC recommended (rec 31-6) that the Government develop and publish a list of laws and binding schemes in force outside of Australia that effectively uphold principles for the fair handling of personal information that are substantially similar to the APPs. The ALRC made it clear that the mere fact that a recipient is subject to a listed binding law or scheme is not determinative in itself, as the entity must still form its own reasonable belief based on the information available to it.

The Government response stated that agencies and organisations will be able to use the list to assist them in forming a reasonable belief that, in the circumstances of their particular cross-border transfer of personal information, the recipient of the information will be accountable. Once armed with the initial information, entities would be in the best position to find out about the specific laws that apply to the overseas recipient, including whether the recipient is bound by existing privacy laws in the overseas jurisdiction that are substantially similar (we understand that some privacy laws, for example in Korea, only apply to certain industry sectors).

The list would, however, be prepared by the Government rather than the OAIC.

Q47 Google (submission 16) noted that APP 8(9)(2)(c) only covers disclosures to an overseas entity, not any subsequent disclosure by that entity which may be required by law in the overseas jurisdiction, and argue that the provision should recognise requirements of foreign law to ensure that Australian entities are not put at risk of being in breach of the Act due to a disclosure by an overseas entity required by a foreign law. Does the department consider that these concerns are adequately addressed by subsection 6A(4) of the current Privacy Act which are to be replicated in the new Act ?

As noted in the answer to question 4, the existing policy achieved by subsection 6A(4) and section 13D of the Privacy Act will be retained in the amended Act to ensure that an act or practice that is done or engaged in outside Australia will not be an interference with privacy if it is required by an applicable law of a foreign country. In the example provided by Google, an Australian entity would not breach the APPs if an applicable foreign law required disclosure of personal information by an entity to whom that information had been disclosed.

Q48 The Law Council of Australia (submission 31) noted concern that two exceptions which are currently provided for under the NPPs have not been included in APP 8. These relate to

when transfer of information is necessary under a contract (NPP 9(c) and (d)). Is there a reason that these exceptions have not been included?

The existing requirements in NPP 9(c) and (d) of the Privacy Act provide that an organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

> (c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or
>
> (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party

The LCA has commented that the consequence of omitting these requirements is that, if an entity needs to disclose personal information which is necessary for the conclusion of the contract with an overseas entity which is not subject to a scheme which is similar to the APPs, the entity will need to obtain consent or to enter into a contract which will ensure the overseas recipient does not breach the APPs.

In partially adopting ALRC recommendation 31-2, the Government accepted that it was not necessary to include an exception relating to fulfilling contractual obligations. In recommendation 31-2, the ALRC stated that, under the 'Cross-border Data Flows' principle, an exception to the concept of accountability should include where an agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or *contract* which effectively upholds privacy protections that are substantially similar to the model Unified Privacy Principles.

The Government response to ALRC recommendation 31-2 stated that the application of contractual obligations on the recipient of the information does not provide an individual with any rights to take action under the contract. It went on to comment that, while contracts are important mechanisms for agencies and organisations to impose obligations upon recipients, they should not provide an exception from the general accountability obligations.

Further, it is clear that in the case of existing NPP 9(c) and (d), which involves a contract between the *individual* and the organisation, or a contract concluded *in the interest of the individual* between the organisation and a third party, that the individual would consent to the transfer of the information. Under the new APP 8(2)(b), consent of the individual is an exception to the general prohibition under APP 8(1).

Australian Privacy Principle 9 – adoption, use or disclosure of government related identifiers

Q49 Submitters are concerned that APP 9 applies only to organisations not agencies as it was argued that agencies have the potential to abuse individual privacy through data matching and in the public health sector. Why is APP 9 limited to organisations? What protections are in place to limit data-matching?

The ALRC considered arguments in favour of extending the application of the 'Identifier' principle to agencies but noted that it could seriously impede activities conducted for a public benefit, including programs designed to reduce fraud and identity theft; service delivery; and research.[16] It also noted that appropriate and important information sharing between agencies would be restricted by the application of the 'Identifiers' principle. The ALRC noted that regulation of agencies for data-matching could be carried out either in separate sectoral legislation or guidance provided by the OPC. As a result of these findings, the Government has not applied the requirements in APP 9 to agencies.

In terms of existing protection in place to limit data-matching by agencies, some agencies are currently subject to data-matching requirements in legislation and in guidelines issued by the Privacy Commissioner.[17]

Q50 Qantas (submission 38, p. 4) recommended the word 'serious' be deleted from the phrases 'serious threat' and 'misconduct of a serious nature', as the word serious is subjective and could cause different views on the interpretation of threat and misconduct. What is your response to this issue?

In its submission, Qantas recommends that the word 'serious' be removed from a number of APPs. It believes that *any* threat to the life, health or safety of a passenger which necessitates the gathering of sensitive information should be sufficient to justify an exception. It illustrates this point in the following example:

> One example in the context of Qantas' activities relates to misconduct of passengers on flights or in terminals who are affected by alcohol and become rude or abusive to staff or other passengers. If these are regular passengers, such as those working in remote areas, it may be necessary to warn their employer that if the conduct continues Qantas will refuse to carry those individuals.

The concept of a 'serious threat' or 'misconduct of a serious nature' was included throughout a number of the APPs consistent with a number of ALRC recommendations (eg see 25-3 and 29-3). The Government has decided to remove the 'imminent' requirement consistent with those recommendations but there was little support or justification demonstrated to the ALRC for the further removal of the serious requirement. The APPs have been developed to address concerns raised by a number of submitters to the ALRC report that the collection, use or disclosure of personal information should not be permitted for minor breaches of professional misconduct.

In the example provided by Qantas, it would be a matter for Qantas to warn the individual in question as a first step and then possibly refuse them further service.

[16] ALRC Report at para 30.34 – 30.35
[17] See more information at http://www.privacy.gov.au/law/other/datamatch

Australian Privacy Principle 10—quality of personal information

Q51 Privacy Law Consulting Australia (submission 24, p. 8) argued that entities adhering to APP 10(2) may be subject to privacy claims by individuals on new grounds ie 'that a decision was made about them taking into account irrelevant information'. Do you consider that this is a possibility?

It would be possible under proposed APP 10(2) for individuals to make complaints about organisations if they did not take such steps (if any) as are reasonable in the circumstances to ensure that the personal information the organisation uses or discloses is accurate, up-to-date, complete and relevant.

That is consistent with ALRC recommendation 27-1, which recommended that both organisations and agencies should have a data quality obligation with a 'relevance' element. The ALRC noted that it would complement the requirement in the 'Collection' principle that personal information collected by an organisation should be 'necessary for one or more of its functions or activities'.[18]

Q52 Why has the term 'relevant' only been used for use and disclosure in APP 10(2) and not in the provisions related to collection as recommended in the ALRC review and the Government's response?

As noted above, there is already an existing requirement in the proposed 'Collection' principle that personal information collected by an organisation should be 'reasonably necessary for, or directly related to, one or more of the entity's functions or activities'. Including 'relevant' in the collection-related data quality principle would have caused confusion with this overarching requirement in relation to collection.

Australian Privacy Principle 11–security of personal information

Q53 Telstra (submission 19, p. 4) suggested that 'interference' could be viewed as 'unlawful interception' which would require further technological protections and 'degrees of encryption' and this could 'unfairly impose responsibility for external events or attacks' on organisations and lose the technologically neutral objective of the legislation. Is this a correct interpretation of the impact of APP 11?

The inclusion of 'interference' in APP 11 is intended to recognise that attacks on personal information may not be limited to misuse or loss, but may also interfere with the information in a way that does not amount to a modification of the content of the information (such as attacks on computer systems). It is correct that this element may require additional measures to be taken to protect against computer attacks etc, but the requirement is conditional on steps being 'reasonable in the circumstances'. Practical measures by entities to protect against interference of this nature are becoming more commonplace.

The use of the term 'interference', which focuses on the activity rather than the means of the activity, ensures that the technologically neutral approach to the APPs is retained.

[18] ALRC Report at para 27.24

Australian Privacy Principle 12 – access to personal information

Q54 Submitters have commented on the language used in APP 12 – that it is loose, vague or overly complex leading to redundant and confusing clauses. Has the department considered these comments and if so, will amendments be made to APP 12?

This single principle is more lengthy and prescriptive than other APPs (eg collection, use and disclosure) for a number of reasons. First, it is intended to consolidate the existing access and correction obligations in IPPs 6 and 7 for agencies and NPP 6 for organisations. It is also intended to clarify the existing overlap between the Privacy Act and the FOI Act, with the provisions and administrative machinery under the FOI Act being, in practice, the primary means for dealing with access and correction requests from individuals. In addition, it was also necessary to outline the separate and broader range of exceptions to access for organisations. Finally, it was necessary to set out the process once a request for access is received.

Australian Privacy Principle 13 – correction of personal information

Q55 APP 13 does not include any reference to the correction of personal information that is misleading as recommended by the ALRC. Why has misleading information not been included in the scope of APP 13?

Under recommendation 29-5, the ALRC recommended a 'misleading' element be included within the 'Access and Correction' principle. That is, if an individual seeks to have personal information corrected under the principle, an agency or organisation must take such steps, if any, as are reasonable to correct the personal information so that, with reference to a purpose for which the information is held, it is accurate, relevant, up-to-date, complete and *not misleading*.

During the course of drafting the provisions, it became clear that it was not necessary to include 'misleading' as it was covered by 'accurate' and 'relevant', and it would create an inconsistency with APP 10 about quality of personal information, in which entities have to ensure the personal information they use or disclose is 'accurate, up-to-date, complete and relevant'.

Q56 Concerns were raised about the administrative burden of APP 13(3) – the notification of correction to third parties. Has the department considered the compliance costs of this provision? Do you think that this administrative burden of provision will discourage some entities from keeping records of disclosure of information to third parties so that it is impracticable for them to comply with APP 13(3)?

The Department believes that the qualifications in APP 13 of 'reasonable steps (if any)' and 'practicability' will provide the necessary flexibility in the obligation to ensure it does not create an onerous compliance burden.

It is anticipated that guidance from the AIC will be necessary to assist agencies and organisations to comply with the obligation. For example, guidance could outline factors for assessing whether it would be reasonable and practicable to notify third parities of a correction, with such factors including the materiality of the correction and the potential consequences for the individual arising from the use and disclosure of incorrect information.

The ALRC Report found factors that should be addressed when assessing whether it would be reasonable and practicable to notify third parties that it has disclosed incorrect information include whether the agency or organisation has an ongoing relationship with the entity to which it has disclosed the information, the materiality of the correction, the length of time that has elapsed since the information was disclosed and the likelihood that it is still in active use by the third party, the number of entities that would need to be contacted by the agency or organisation and the potential consequence for the individual of the use and disclosure of the incorrect information.[19]

3. OTHER ISSUES

Section 19 – Extra-territorial operation of the Act, etc

Q57 The Law Council of Australia (submission 31, p. 8) has stated that disclosure under compulsion of a foreign law may contravene the requirement of the new Privacy Act and has recommended that disclosures under any law or legal process applicable to the organisation should be expressly permitted. What is your response to the Law Council's recommendation?

The exposure draft APPs is just one part of the process of amending the Privacy Act. As noted above, the Government intends for disclosure by organisations with an Australian link (as per s 19(3)) under foreign law to be a valid exemption from the operation of s 9(1).

Provisions for the operation of foreign law in this way are currently enacted in section 13D of the Privacy Act. Since the policy intent behind these provisions has not changed, they have been replicated in the new APPs. Some minor issues relating to the definition of the law of a foreign country need to be resolved before this takes place, but these will be further revised in the reforms before they are brought before the Parliament.

Q58 How will proposed section 19(3)(g) apply to international internet services? Where does the 'collection' take place – in Australia or at the place at which the information is collated and processed? Will the place of collection impact on the application of the proposed Act?

International internet services, such as entities engaged in online retail that sell to Australians, would be required to comply with the APPs so long as they fulfilled both branches of paragraph 19(3)(g). It is likely that sub-paragraph 19(3)(g)(i) would capture businesses operating in Australia, but not businesses operating in foreign jurisdictions that happen to engage in commerce incidental to their primary purposes with customers in Australia.

Collection takes place for the purpose of the Act when data is entered in Australia, regardless of the point of collation or processing. As such, the place of collection affects whether the Act applies, and once collection takes place s20, which sets out rules and responsibilities relating to the disclosure of personal information to an overseas recipient would apply with regard to acts or practices concerning the data collected.

[19] ALRC Report [para 29.132]

Section 20 – Acts and practices of overseas recipients of personal information

Q59 The Australian Association of National Advertisers (submission 21) recommended that section 20 be amended to include exemptions to deal with mitigating factors. Do you have a view on this recommendation?

The AANA recommendations are based on concerns about the unauthorised disclosure of personal information that has been lawfully transferred to a foreign entity via a breach of that foreign entity's data security. The example given by the AANA would not, under the new Privacy Act, be a breach of s 20 as the breach and disclosure would not be an 'act or practice' of the foreign entity.

The accountability of organisations which choose to transfer data across borders as provided for in s 20 is a necessary condition for the security of that data. Contracts in place between two entities involved in a cross-border transfer of data do not provide adequate protections for the individuals to whom the information pertains. As such, contracts are not an acceptable mitigating factor for the purposes of s 20.

Q60 The Law Council (submission 31) suggested that the liability imposed by section 20 be limited in time and aligned with other statutory limitation periods. Is there a limitation period for the application of section 20? If not, would it be beneficial for such a limitation to be included in the Act?

There is not currently any statutory limitation relating to the 'interference of privacy' that may occur under s 20. As the Act has not previously envisaged judicial enforcement (consistent with the principles-based nature of the Privacy Act), limitation periods have not been a relevant factor.

However, the ALRC has made a number of recommendations that the AIC be given stronger enforcement powers, eg. the power to commence proceedings in the Federal Court or Federal Magistrates Court for enforcement orders and civil penalties. The Government has either accepted, or accepted in-principle, these recommendations, and will be developing draft amendments to address these issues. Relevant civil litigation rules that underpin this system, including statutory limitation periods, will be considered as part of the development of these amendments.