Attorney-General's Department

Response to Senate Standing Committee on Legal and Constitutional Affairs Questions on Notice

Australian Privacy Principles

- **Submitters such as the OAIC and the Law Council (p. 4) have criticised some of the exceptions granted to government agencies under the APPs, arguing that the different standards for government and non-government entities are unnecessary and undesirable. Has the intent of creating a single set of principles for all Australian entities been nullified by the inclusion of different standards in several of the APPs for government and non-government bodies?**

There has been careful consideration given to the inclusion and breadth of agency specific provisions in the proposed APPs. While the general approach has been to apply the single set of principles to all entities, in some cases there is a clear rationale for applying separate rules.

First, there are particular APPs that apply only to the activities of a specific type of entity. . For example, as recommended by the Australian Law Reform Commission, APP 7 (direct marketing) and APP 9 (government related identifiers) apply only to organisations. The Law Council of Australia (LCA) has noted that certain *Commonwealth Authorities and Companies Act 1997* agencies will need to comply with APPs 7 and 9 in relation to their commercial activities as a result of the application of section 7A of the Privacy Act. The policy rationale underpinning is that, where such agencies undertake these types of activities, they should be required to comply with the same privacy requirements as their private sector competitors.

In addition, the Privacy Act does not prescribe two sets of rules relating to direct marketing and government related identifiers. There is only one set of rules in the Privacy Act applying to those activities, and, if an entity is not regulated by those rules, the Privacy Act does not apply to them in relation to those activities.

The Office of the Australian Information Commissioner (OAIC) has suggested that exceptions permitting specific handling activities of certain agencies should be included in relevant portfolio legislation or in a Public Interest Determination (PID), rather than the APPs.

While portfolio legislation will normally provide the lawful authority for an agency to undertake certain powers, functions and activities, it is also necessary in exceptional circumstances to include specific exceptions in the APPs to make clear that specific activities of agencies will not contravene APPs obligations. Some of the exceptions have been included to provide additional certainty about the operation of the APPs on legitimate activities undertaken overseas, including those in urgent or emergency situations. Others preserve existing exceptions in the Information Privacy Principles (IPPs), eg. which enable the collection, use/disclosure etc of personal information for law enforcement purposes.

Definition of 'consent'

- **Submitters such as the Law Institute of Victoria (p. 3) and the NSW Privacy Commissioner (p. 6) have questioned whether the current definition of 'consent' in the Privacy Act provides enough protection for individuals, particularly where implied consent is relied on to gather or use personal information.**
    - **Has the Department considered updating the definition of 'consent' in the Privacy Act, and does it think any changes are necessary?**
    - **Submitters have argued the possibility for entities to rely on 'implied consent' in the context of APP 3.3 and APP 7.4 is inappropriate. Do you agree?**

The ALRC extensively considered the issue of 'consent' under the Privacy Act, including whether the definition should be amended (Ch 19). In terms of the best approach to clarifying the meaning of 'consent', the ALRC did not support amending the Act in detail to outline what was required to obtain consent, noting that this approach would require a very large number of prescriptive rules. Instead, the ALRC recommended that the OAIC should develop and publish further guidance about what is required of agencies and organisations to obtain an individual's consent under the Privacy Act (Rec 19-1). 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'. The Government response accepted this recommendation and encouraged the development and publication of appropriate guidance on this issue by the OAIC.

The Senate Finance and Public Administration Legislation Committee (SFPALC) considered the same issue and came to a similar conclusion as the ALRC. The SFPALC recommended that the OAIC develop guidance on the meaning of 'consent' in the context of the Privacy Act as a matter of priority (rec 4). In response to that recommendation, the Government agreed that OAIC guidance on the meaning of 'consent' would be useful to provide clarity to entities and individuals about the application and operation of that term.

Given the clear recommendations of the ALRC and the SFPALC, the definition has not been changed, nor has there been any inclusion of separate 'express' or 'implied' consent provisions. The Department anticipates that issue of how consent, including implied consent, operates in the context of APP 3.3 and APP 7.4 will be the subject of OAIC guidance.

Proposed new sections 16A and 16B

- **Why have 'permitted health situations' and 'general health situations' (proposed new sections 16A and 16B of Schedule 1) been placed in separate provisions rather than in the APPs themselves?**

Proposed section 16A (Permitted general situations etc) and section 16B (Permitted health situations etc) were included as a result of a recommendation of the SFPALC that the draft APPs be reassessed with a view to the use of simpler and more concise terms and to avoid the repetition of requirements that are substantially similar.

The inclusion of the tables in proposed new sections 16A and 16B has resulted in a reduction in the length of the APPs and the avoidance of repetition. For example, a number of the exceptions in the table in proposed section 16A are applicable to APPs 3, 6 and 8.

Australian Privacy Principle 2

- **APP 2.1 states that 'individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter'. Submitters have claimed that this wording allows entities to provide options for either anonymity or pseudonymity, rather than both.**
    - **Is the policy intent behind this provision to allow entities to provide options for either anonymity or pseudonymity, or is it intended that entities should be obliged to provide both options where lawful and practicable?**

The policy intent behind APP 2 is that entities are obliged to provide both the options of anonymity or pseudonymity where lawful and practicable. That is, an entity will not comply with APP 2 if it offered only pseudonymity, where the option of anonymity would also be lawful and practicable in the circumstances.

The ALRC considered the inclusion of pseudonymity as providing a more flexible application of the principle because it would cover:

> "…the situation where it would be impracticable or unlawful for an individual to transact anonymously but where these barriers would be overcome if the individual were to transact pseudonymously with an agency or organisation." (Para 20.25, page 696).

The ALRC believed that the decision of an agency or organisation to provide an option to interact anonymously or pseudonymously will be guided by the particular context. Generally speaking, where the agency or organisation has no need to contact the individual in the future, anonymity would be the most appropriate option. Where some form of identifier is required but need not be personal information, pseudonymity is likely to be appropriate.

To provide additional clarity about the operation of APP 2, the ALRC also recommended that OAIC guidance be developed that, amongst other things, outlines the difference between providing individuals with the option to interact anonymously and pseudonymously. The Department believes that this additional guidance will promote greater awareness amongst entities about the appropriate circumstances in which it should offer the option of anonymity or pseudonymity.

The Government accepted the ALRC's recommendations on anonymous and pseudonymous transactions, which are reflected in APP 2.

- **If entities are intended to be obligated to provide both options, does APP 2.1 need to be reworded to make this objective clear?**

The Department believes that it is clear that APP 2 obliges entities, where lawful and practicable, to provide both the option of anonymity or pseudonymity. APP 2 begins by

stating that 'individuals must have the option of', rather than beginning along the lines of 'an entity must offer the options of either', suggesting that an individual must have the right to select from two options. Secondly, the use of 'or' in APP 2 between 'not identifying themselves' and 'of using a pseudonym' is a reference to the fact than an individual may, if taking up one of the offered options, operate either anonymously or pseudonymously. It is not a reference to an entity offering one or the other.

In addition, as noted above, it is anticipated that OAIC guidance will be developed that will provide detailed information about the operation of APP2, including information about when both options should be offered, and where it may be impracticable to offer one of the options.

- **APP 2.2(b) states that the obligations in APP 2.1 do not apply where it is impracticable for an APP entity to deal with individuals 'who have not identified themselves'. Facebook, Google, IAB Australia and Yahoo!7 submitted that this wording does not adequately address the issue of pseudonymity, and suggests that the provision should be reworded to refer to 'individuals who have not identified themselves or who use a pseudonym' to ensure that pseudonymity is covered in this exemption.**
  - **What is your response to this suggestion?**

Under APP 2.1, an individual must be given the option of anonymity or pseudonymity when dealing with an APP entity in relation to a particular matter. APP 2.2 recognises that this right is not absolute and that particular exceptions apply. Where those exceptions apply, an APP entity is not required to offer the option of the anonymity or pseudonymity. An example of where an exception will apply is where a law enforcement agency is investigating a criminal offence and requires a person's identity to assist in that investigation.

The Explanatory Memorandum makes it clear that the option of anonymity or pseudonymity is not available if an exception under APP 2.2 applies. That is, an APP entity will not be required to comply with APP 2.1 'where it is impracticable for the entity to deal with individuals who have not identified themselves (ie where an individual seeks to remain anonymous or uses a pseudonym)'. If it is impracticable for an entity to offer the option of a pseudonym unless they obtain identification details from the individual, the entity is not required to provide that option.

The suggestion put forward by some submitters is that clarity could be enhanced in this exception if it specifically referred to the impracticality of providing a pseudonym. The Government is considering options to enhance clarity around the application of this exception.

Australian Privacy Principle 3

- **Submitters such as the NSW Privacy Commissioner and the Law Council of Australia have argued that agencies and organisations should be subject to the same requirements regarding the collection of personal information, and that the 'directly related to' test for agencies should be deleted from APP 3.1 and APP 3.3.**

- **What is your response to these suggestions? Why has the 'directly related to' test been retained for agencies, and why do agencies need this additional test along with the 'reasonably necessary for' criteria for collecting personal information?**

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.

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.

Agencies are also subject to stricter oversight and accountability arrangements through Parliament, the Executive and the Ombudsman.

- **Facebook, Google, IAB Australia and Yahoo!7 submitted that in many instances internet services based outside of Australia collect personal information from persons inside Australia, and that further clarification is needed to make it clear that these overseas entities are not subject to the requirement of the APPs.**
    - **What is your response to this concern? How is the collection of personal information from individuals located in Australia by overseas entities to be treated under the APPs?**

The Government's policy intention is that entities carrying on business in Australia or an external Territory should be subject to Australian laws. Entities that provide online services may also have a physical presence in Australia. Where this is relevant, this question will need to be considered in all the circumstances and the location of the internet services outside Australia (for example, the location of servers in a foreign jurisdiction) will be one of the issues to consider, along with other matters. However, it is also the case that an entity can carry on business in Australia without having a physical presence in Australia. The question of whether an overseas entity is carrying on business in Australia is addressed by section 5B, which deals with the extra-territorial operation of the Privacy Act, and in particular subsection 5B(3). The intention is that the location of an entity that does business in Australia should not be a basis for the entity avoiding obligations and responsibilities under the Privacy Act to individuals in Australia. An individual in Australia should benefit from the protection provided to their personal information by the Privacy Act and entities should be accountable for, and responsible to, individuals for providing the appropriate protection.

The Explanatory Memorandum makes it clear that the collection of personal information 'in Australia' under paragraph 5B(3)(c) of the Act includes the collection of personal information from an individual who is physically within the borders of Australia or an external territory, by an overseas entity.

The Explanatory Memorandum further states that a collection is taken to have occurred 'in Australia' where an individual is physically located in Australia or an external Territory, and information is collected from that individual via a website, and the website is hosted outside of Australia, and owned by a foreign company that is based outside of Australia and that is not incorporated in Australia.

It is intended that, for the operation of paragraphs 5B(3)(b) and (c) of the Privacy Act, entities that have an online presence and collect personal information from people who are physically in Australia, carry on a 'business in Australia or an external Territory'.

- **Salmat argued (submission 26, p. 10) that the legitimate activities of outsourced service providers in collecting personal information on behalf of a client are not adequately catered for under APP 3.6.**
    - **Is it the intent of the bill that outsourced third party service providers will not be able to collect personal information from individuals on behalf of a client?**
    - **Will such activities be covered under the exemption in APP 3.6(b), which allows collection by a third party where it is 'unreasonable or impracticable' for an organisation to collect personal information from an individual directly?**

The obligation in APP 3.6(b) is exactly the same as the existing obligation that private sector organisations, including third party service providers, have under National Privacy Principle 1.4.

Where Salmat is collecting personal information directly from an individual, it is the collecting entity and would have to meet the obligations under APP 3. Under APP 6, Salmat could then disclose that information to a third party client who has requested the collection, since that was the primary purpose of the collection. That third party client would not have obligations under APP 3 since it has not directly collected the information. Salmat's handling of personal information under the key relevant APPs (ie 3, 5 and 6) before that information was disclosed to its client, is a matter for Salmat rather than its client.

Where the client has received the personal information from Salmat, it would then be required to handle it in accordance with the APPs.

Australian Privacy Principle 4

- **The NSW Privacy Commissioner noted that members of the public may in some instances prefer to have their information returned to them rather than destroyed or de-identified. It recommended that APP 4 be amended to include the option of returning personal information to the individual, and that APP 4 also be amended to allow entities to involve the individual in decisions about what happens to their unsolicited personal information, where this is practicable and appropriate.**
    - **What is your response to this suggestion?**

APP 4.2 provides that an entity may use or disclose unsolicited personal information it has received for the purposes of determining under APP 4.1 whether it could have collected the information. Under this provision, there would be nothing to prevent an entity from

approaching the individual concerned and disclosing the personal information to that individual. That could be done for the purpose of determining whether the individual would have consented to the collection. Given that this option is available to an entity, there would appear to be no need to amend APP 4 to implement the NSW Privacy Commissioner's suggestion.

In some circumstances, it may not be lawful or practicable to take this approach. As the ALRC noted, an entity may have no option but to retain personal information because of records retention legislation, or accountability, audit or evidentiary requirements (para 21.53).

Australian Privacy Principle 6

- **The Law Council argued that APP 6.2(d), which allows an organisation to use or disclose personal information for a secondary purpose if a permitted health situation exists, should be extended to apply to agencies as well.**
    - **What is your response to this argument? Why does APP 6.2(d) apply only to organisations and not agencies?**

The Bill is not intended to change the effect of the health privacy related provisions that currently operate under the National Privacy Principles. Those provisions have been replicated throughout the new APPs, including APP 6.2(d). Implementation of the Government's response to the ALRC's recommendations on the health privacy related provisions, including the operation of APP 6.2(d), will be considered at a later date.

- **With regards to the exception for sharing biometric information and templates found in APP 6.3, the OAIC noted that APP 6.2 already creates an exception for information sharing where an agency reasonably believes that the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body. The OAIC therefore argued that the exception in APP 6.3 is unnecessary.**
    - **What is your response to the issues raised by the OAIC in regards to APP 6.3?**

The policy intention of APP 6.3 is to enable non-law enforcement agencies to disclose biometric information and templates for a secondary purpose to enforcement bodies where an APP 6 exception, including the enforcement related activity exception, is not applicable. This may occur where the disclosure is for purposes such as identity/nationality verification or general traveller risk assessment, in circumstances where there is a legitimate basis for the disclosure but no criminal enforcement action is on foot.

As the purposes for disclosure may vary or increase, particularly into the future, it is important to have the safeguard of Privacy Commissioner oversight through the development of guidelines. As with existing data-matching guidelines, these could relate to requirements relating to monitoring, transparency and technical matters.

The proposed guidelines will provide an additional layer of privacy protection for biometric information and templates. This type of information is already included in the definition of 'sensitive information' and therefore subject to additional safeguards under other

requirements in the APPs. For example, such information may not be collected by an APP entity without consent, unless specific exceptions in APP 3.3 apply.

The policy rationale in APP 6.3 recognises that non-law enforcement agencies have current, and will have future, legitimate reasons to disclose biometric information and templates to enforcement bodies, but that this should occur within a framework that protects against improper disclosure.

Australian Privacy Principle 7

- **Submitters such as the Australian Direct Marketing Association and the Fundraising Institute of Australia have argued that the description of APP 7 as a 'prohibition' on direct marketing will cause confusion and uncertainty among the public and businesses, because direct marketing is still allowed under the principle in a variety of circumstances.**

    - **What is your response to these concerns, and why has the approach been taken to describe APP 7 as a 'prohibition'?**

The approach in Australian Privacy Principle (APP) 7 of casting the principle as a 'prohibition' against certain activity followed by exceptions is a drafting approach used in principles-based privacy regulation to clearly identify the information-handling activity that breaches privacy, followed by any exceptions to this general rule that would permit an entity to undertake the activity. This is consistent with the practical effect of the current Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs). For example, both IPP 1 and NPP1 begin by expressly stating that the collection of personal information is not permitted unless certain exceptions apply.

In the case of APP 7, this approach was implemented as a result of comments made by the Senate Finance and Public Administration Legislation Committee, which recommended that APP 7 should be re-drafted to simplify terminology and clarify the intent of the provision. Consistent with the clearer approach taken with other provisions in the Bill, particularly relating to credit reporting (eg see proposed sections 20C and 20E), the heading 'Prohibition' was included.

- **Why does the Bill not include a definition of the term 'direct marketing'? Would a clear definition help provide clarity as to the scope of APP 7?**

The ALRC specifically considered whether a definition of 'direct marketing' should be included in the APPs and decided that it should not. The ALRC found that there was no consensus about how the term should be defined. It further found that providing a definition of direct marketing may limit the application of the principle, noting that if practice later evolves, new methods of direct marketing may not be caught by the definition.

The Government agreed with this approach, which is reflected in the Bill.

For additional clarity, the Explanatory Memorandum includes a description of direct marketing practices based on descriptions used in the past by the ALRC and the OAIC. The EM notes that this could include communicating directly with consumers to promote the sale of goods and services through mail, telephone, email and SMS. The risk with including a

narrower description is that it may become out-of-date with the development and use of new technologies.

- **Facebook, Google, IAB Australia and Yahoo!7 argued (submission 39, p. 6) that the wording of APP 7.2(c) and APP 7.3(c) requires an organisation to give individuals a simple means to opt-out of all direct marketing communications, rather than just direct marketing communications which use the individual's personal information.**

    - **Is this interpretation consistent with the intent of these provisions?**

    - **Do these provisions need to be reworded to refer to direct marketing communications which relies on the individual's personal information?**

The intended scope of APP 7 is to regulate direct marketing activity that involves the use or disclosure of personal information. That is, it involves use or disclosure of 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'. The policy rationale in APP 7 is that organisations that undertake direct marketing involving the use and disclosure of personal information of particular individuals should be allowed to do so, but only where those individuals are given the choice to opt out of this form of direct marketing.

APP 7 will not cover forms of direct marketing that are received by individuals that do not involve the use or disclosure of their personal information, such as where they are randomly targeted for generic advertising through a banner advertisement or generic 'pop up' ads. Nor will APP 7 apply if it merely targets a particular internet address on an anonymous basis for direct marketing because of its web browsing history. These are current online direct marketing activities that will not be affected by the amendments.

- **Some submitters have claimed that the requirement to include an opt-out statement in each direct marketing communication under APP 7.3(c) is not possible in some marketing channels such as social media and online banner advertisements.**

    - **What is your response to this suggestion?**

The effect of APP 7 is that, where an organisation is directly targeting an individual by using or disclosing personal information, it must provide an opt-out mechanism under APP 7.2 or 7.3. Opt out mechanisms are available and used for many existing types of communications over the internet. The Department does not believe it would not be unduly onerous or technically difficult for direct marketers who directly target an individual by using or disclosing their personal information to develop and implement a mechanism that allows those consumers a choice to opt out of that activity. The opt out requirements are designed to operate flexibly so that organisations can develop an appropriate mechanism tailored to the particular form of advertising they are undertaking, while raising sufficient awareness amongst consumers of their right to opt out, and the means by which they can easily do so. While the Department notes that lengthy opt out messages may be impractical in some circumstances, there may be shorter messages (eg 'opt-out' with a link) that could be considered.

The principle will require organisations to adapt to new direct marketing rules that enhance the privacy protections of consumers. Shifting the balance more in favour of consumers may require an additional mechanism to be developed.

Australian Privacy Principle 8

- **The Australian Privacy Foundation has argued that it will be impossible in practice for an individual to prove on the balance of probabilities that an overseas recipient has committed a breach of the APPs in relation to their personal information.**
  - **How do you envisage individuals being able to prove that a breach of the APPs has been committed by an overseas recipient? Does the Privacy Commissioner have a role to play here?**
  - **Should a 'rebuttable presumption' be introduced, such that the burden of proof fall upon an organisation to prove that a breach has not occurred?**

Question (a)

The complaint process is that an individual may complain about an act or practice that may breach the APPs. While individuals will be encouraged to provide as much detail as possible, individuals will not be required to specify the APP which they suspect has been breached. There is no special or different complaint process where a breach may have been committed by an overseas recipient.

Investigation of complaints is the role of the Information Commissioner. When making judgements about facts, administrative decision makers like the Commissioner make those judgements in terms of the civil standard of proof, the balance of probabilities. For the Commissioner to decide that a breach of privacy has occurred he needs to be satisfied, on the basis of all the relevant evidence, that it is more likely than not that a breach did occur. That satisfaction may arise in a number of ways, for example due to evidence from either party or a failure of a respondent to prove the application of an exception.

As set out in the note to the provision, APP 8.1 operates in conjunction with section 16C to provide that an act or practice of an overseas recipient is taken to have been done or engaged in by the APP entity. Consistent with the current provisions, an individual will be required to identify the respondent to the complaint. The operation of APP 8.1, in conjunction with section 16C, means that it will not be necessary for an individual to identify the overseas recipient of the personal information as part of their complaint. The individual will only need to identify the relevant APP entity. The APP entity will be responsible (that is, accountable) for the acts and practices of the overseas recipient. In investigating a complaint the Office of the Information Commissioner will consider the facts of the case, which will assist in determining which, if any, possible breaches of the APPs need to be considered. Where necessary, the investigation will also consider the acts or practices of the overseas recipient.

An individual may also wish to make a complaint about an APP entity breaching a particular APP. APP 8.1 requires an APP entity to undertake certain steps before any personal information is disclosed to an overseas recipient. A complaint about a breach of APP 8.1 would be investigated by the Office of the Information Commissioner.

Question (b)

The Department does not consider that a 'rebuttable presumption' is necessary or appropriate. The Commissioner's powers and functions have been reviewed and the Amendment Bill

contains appropriate reforms to the Commissioner's powers and functions. Once a complaint is received, a complainant does not need to discharge a burden of proof for the complaint to be investigated.

It is a matter for the Commissioner to conduct an investigation into a complaint using the range of powers available. For example, the Commissioner has powers to conciliate complaints, to make preliminary inquiries of any person, to require a person to provide information or documents, or to attend a compulsory conference. After investigation, the Commissioner may make a determination in relation to the investigation. As mentioned above, for the Commissioner to decide that a breach of privacy has occurred he needs to be satisfied, on the basis of all the relevant evidence, that on the balance of probabilities a breach did occur.

Credit reporting

- **The Law Institute of Victoria questioned whether the Bill will enhance individuals' right to privacy as 'the Bill seeks to regularise current business practices with limited provision for the rights and interests of individuals and fundamental principles of privacy' (*Submission 8*, p. 2). What is your response?**

The Department does not agree with the opinion of the Law Institute of Victoria.

The purpose of the credit reporting provisions is to balance, on the one hand, the need for credit providers to have access to sufficient personal information to adequately assess an individual's credit worthiness and make effective credit risk decisions against, on the other hand, the interests of individuals in limiting the collection, use and disclosure of their personal information. The Government has considered both the recommendations of the ALRC and the submissions and views of a wide range of stakeholders in striking an appropriate balance in the area of credit reporting. The protection of personal information is at the forefront of the Government's commitment to reform the credit reporting system. The Government response to ALRC recommendation 54-3 stated that:

> The policy framework for credit reporting regulation should be to protect a subset of personal information which is maintained by credit reporting agencies and disclosed to credit providers for the purpose of assessing an individual's eligibility for credit. This framework will ensure that any personal information collected, used and disclosed within the credit reporting system will be afforded specific and appropriate protection.

In accepting the ALRC's recommendations to introduce more comprehensive credit reporting, the Government considered that the reforms to create a more effective credit reporting system would significantly benefit Australia while maintaining strong and effective privacy protections. The Government response to ALRC recommendation 55-1 stated that:

> Greater access to the five data sets as proposed by the ALRC will allow more robust assessment of credit risk, which in turn could lead to lower credit default rates. On balance, comprehensive credit reporting is also likely to improve competition in the credit market, which will result in benefits to both individuals and the credit industry.

The Government response to ALRC recommendation 55-1 went on to state that the Government 'considers that the enhanced notification, data quality and dispute resolution requirements will provide sufficient protections to prevent the misuse of this information.'

The Department's view is that the proposed credit reporting provisions effectively implement these Government commitments. The provisions impose strict controls on the collection, use and disclosure of personal information in the credit reporting system. Credit reporting bodies and credit providers are subject to enhanced obligations in relation to notification, data quality and dispute resolution. The provisions enhance and simplify the access and correction procedures and the complaints processes for individuals. In relation to the particular points made by the LIV in support of their comment, the Department has the following observations:

- Individuals are, for the first time, provided with effective mechanisms to deal with the consequences of identity theft. The ban period has been increased from 14 to 21 days following the Government's acceptance of recommendation 10 of the Senate Finance and Public Administration Legislation Committee in its report on the credit reporting exposure draft.
- The use of credit reporting information for direct marketing is prohibited. The use of strictly limited types of credit reporting information for pre-screening purposes is tightly controlled and subject to opt out mechanisms that are consistent with the more general obligations in APP 7 in relation to direct marketing.
- Individuals are guaranteed free access to their credit reporting information every 12 months, with additional access subject to a requirement that access charges, if any, are not excessive. The requirement that access charges must not be excessive is identical to the requirements in relation to charges for access to an individual's personal information under the APPs. APP 12 deals with access to personal information (outside the credit reporting system). APP 12.7 prohibits agencies from charging for access. However, there is no free right of access to personal information held by organisations. APP 12.8 states that, if an organisation charges for access, the charge must not be excessive.
- Written notes are required to provide a record of certain uses and disclosures in appropriate circumstances. Imposing additional notification requirements when a written note is made, as suggested by the LIV, would impose a significant burden on industry without any clear benefit to the individual. Written notes are required to ensure evidence of permitted uses or disclosures. A written note will not reveal 'inappropriate' uses or disclosures – the written note will provide evidence of a use or disclosure pursuant to a particular provision. A requirement to notify an individual each time a written note is made would be impracticable. Obligations to make written notes are set out in subclauses 20E(5), 20G(7), 20H(3), 20H(6), 20Z(5), 20ZA(4), 21D(6) and 21G(6). The effect of these provisions is that credit reporting bodies must make a written note of <u>every</u> disclosure, and most uses, of credit reporting information, while credit providers must make a note of disclosures to a credit reporting body or <u>every</u> use and disclosure of credit eligibility information. In many cases, a notification requirement would have the effect of notifying an individual that a written note of a disclosure has been made in relation to a use or disclosure that the individual already knows about – for example, where the use or disclosure occurs as a result of the individual submitting an application for consumer credit.

- **The Law Council of Australia expressed concern about certain structural elements of the Bill as it relates to the regulation of credit reporting: for**

example, 'the structure whereby key concepts are defined in several places within the Bill but distant from the Part IIIA context in which they are used' (Submission 14, p.11). Do you consider that the drafting style used in the Bill might confuse consumers and therefore be counterproductive?

The Government accepted ALRC recommendation 5-2 that the Privacy Act should be redrafted to achieve greater logical consistency, simplicity and clarity. The Government noted this would provide an opportunity to redraft the Privacy Act to make it more user-friendly for individuals, organisations and agencies. The Department has worked to implement this recommendation throughout the Privacy Amendment Bill, including the credit reporting provisions. The Department considers that the drafting style adopted in the Bill reflects current best drafting practice.

The credit reporting provisions must provide clear and direct guidance to credit reporting bodies, credit providers and other interested entities on their obligations in relation to personal information in the credit reporting system. The provisions must also clearly identify the rights of consumers and the corresponding obligations on entities. The Department considers that the Bill effectively balances these priorities in its structure and drafting.

It is expected that the principal source of privacy advice and information for consumers will be the Office of the Information Commissioner, including through the Office's website. In addition to the Commissioner's general education functions, the Department notes that the Government's first stage response to the ALRC's report accepted many recommendations that the Information Commissioner provide guidance on the operation of the new Privacy Act. The Department also notes recommendation 6 of the Senate Finance and Public Administration Committee report on the credit reporting exposure draft, which stated that the OAIC should consult with industry and consumer advocates to provide guidance on any consumer education campaigns in relation to the new credit reporting system. The Government response accepted in principle this recommendation, noting that the Government encourages the OAIC to implement this recommendation.

Consistent with modern drafting practices and the approach adopted throughout the Bill, each division in Part IIIA that deals with substantive rights and obligations commences with a guide to assist the reader understand the content of the Division. In addition, clause 19 sets out a guide to Part IIIA as a whole. Guides were not inserted for Division 6 (which contains certain offences) or Division 7 (which deals with certain court orders) as these divisions are short and self-explanatory.

In relation to the structure of the Bill, these privacy law reforms proceed by amending the existing Act, rather than by replacing the Act with an entirely new Act. This means that the structure of the final consolidated Act will remain consistent with the existing structure of the Act. Credit reporting definitions will be located in Part II - Interpretation, which currently contains all definitions and other provisions relevant to interpreting the Act.

At present the credit reporting related provisions are in a number of different places in Part II of the Act. The Bill reorganises the definitions in Part II into a logical sequence and groups similar specific definitions together. Part II will be divided into two divisions – Division 1 will contain all the general definitions for the Act, while Division 2 will contain key definitions relating to credit reporting. Division 1 will include all the credit reporting definitions in subsection 6(1). Where terms require a more comprehensive definition, the reference in subsection 6(1) will point to the specific definition in Division 2. In this way, Division 1 will be the starting point for identifying and locating all defined terms in the

amended Act. The Department considers that this approach to structuring the credit reporting provisions is consistent with the existing structure of the Act and, once amended, will be logical, straightforward and clear.

The Law Council of Australia, in commenting on the style and structure of the credit reporting provisions, also submitted that:

> The Committee considers the use of multiple different named categories of credit-related information (such as credit reporting information, credit information, and credit eligibility information) may over-complicate the drafting. It is submitted that individual data elements may fall into one of these categories when originally collected, but may develop additional characteristics as they are used by a credit provider. (Submission 14, page 11).

The Explanatory Memorandum provides a detailed introduction to the credit reporting provisions at pages 90 to 100. Diagrams representing information flows in the credit reporting system and the relationship of the key terms used to refer to personal information in the credit reporting system are included. The key terms used are credit information; credit reporting information, and credit eligibility information. These three terms are clearly related to each other, describe personal information at different points in the credit reporting system, and are used to precisely define the rights and obligations that attach to the personal information as it is collected, used, disclosed and held by credit reporting bodies, credit providers, or other parties. As noted by the Law Council's submission, the fact that data elements combine with additional data elements as they move through the credit reporting system means that it is important to use clear, precise and distinct terms.

FURTHER INFORMATION ON SERIOUS CREDIT INFRINGEMENT

At the Public Hearing on Tuesday 21 August 2012 the Department was asked a number of questions about serious credit infringement. We understand they related to whether an individual who incurred a serious credit infringement as a consequence of defaulting due to suffering a natural disaster would be able to have the serious credit infringement corrected or removed. The questions also related to hardship variations. The Department provides the following additional information on serious credit infringement and hardship variations of consumer credit obligations.

Summary

Consumer rights set out in the Bill to make a correction request or to make a complaint will apply to any personal information held by a credit reporting body or a credit provider, including personal information relating to a serious credit infringement. In addition, a consumer has the right to complain to the Information Commissioner about a serious credit infringement. Hardship variations of consumer credit contracts are permitted by the National Consumer Credit Protection Act. Hardship variations cannot be listed as part of an individual's credit reporting information. The Government is concerned that permitting the listing of hardship variations may act as a deterrent to individual's seeking hardship variations in appropriate circumstances (including following a natural disaster) and this would be contrary to the intention of providing the right to request a hardship variation.

Development of the definition of serious credit infringement

The definition of serious credit infringement will be inserted in subsection 6(1) of the Act and modifies the existing definition (see item 63 of schedule 2 of the Bill). The definition has three limbs – two deal with suspected fraudulent activity, while the third deals with situations where an individual has failed to pay and the credit provider cannot contact the individual. The ALRC considered the three limbs of the definition of serious credit infringement and recommended that all be retained, noting that failure to pay and then losing contact with a credit provider was a more serious matter than a simple default. The Government accepted ALRC recommendation 56-6 and modified the definition to require credit providers to take reasonable steps to contact an individual where a reasonable person would consider the individual does not intend to comply with their credit obligations. This definition was included in the credit reporting exposure draft that was considered by the Senate Finance and Public Administration Committee. A number of submissions to the Finance and Public Administration Committee proposed a different approach to serious credit infringement.

A number of industry representatives and consumer advocates proposed (known as 'the Veda proposal') abolishing the definition of serious credit infringement on the basis that the first two limbs of the definition are rarely used by industry and the third limb could be replaced with a new concept of 'un-contactable default' which would be retained for 7 years. However, once a person made contact with the credit provider their failure to pay would be listed as a standard default and retained for 5 years.

This proposal was not supported by the Senate Committee's report. However, the Committee recommended that:

> . . . consideration be given to a change of approach in dealing with serious credit infringements to allow for those listings, not relating to intentional fraud, to be dealt with in a different manner (recommendation 8).

The Committee did not recommend a particular approach be taken in this regard. The Government accepted the Committee's recommendation, and stated that the definition of serious credit infringement would be amended to require that six months must have elapsed since the provider last had contact with the individual before an act can be considered to be a serious credit infringement. It was intended that this would provide a sufficient period to allow an individual to become aware of any overdue payments (including through having any such overdue payments listed as a default after 60 days) and to contact the credit provider to make appropriate arrangements.

The Department notes that the credit reporting code of conduct (referred to in the Bill as the CR code) will contain further obligations in relation to serious credit infringement. In particular, the CR code will provide further requirements and guidance in relation to the reasonable steps that a credit provider must take to contact an individual. This may include requirements relating to the number of attempts to contact the individual and other related matters. The CR code will be developed by credit reporting stakeholders, and it is expected that privacy and consumer credit advocates will participate in the development of the CR code before it is submitted to the Information Commissioner for consideration.

Correction of, and complaints about, serious credit infringements

Individuals have rights to make a correction request (clause 20T in relation to credit reporting bodies and clause 21V in relation to credit providers) and to make complaints (Division 5, clauses 23A to 23C in relation to both credit reporting bodies and credit providers). Accordingly, an individual has the right to make a correction request in relation to a serious credit infringement or to make a complaint in relation to a serious credit infringement.

The Department considers that a correction request could relate to any of the elements of the definition of a serious credit infringement, on the grounds that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading. The Department considers that a complaint about an act or practice of a credit reporting body or a credit provider could relate to a serious credit infringement.

The general obligations about the quality of personal information set out in clause 20N (for credit reporting bodies) and clause 21Q (for credit providers) apply to serious credit infringement information as well. These provisions include the obligations to ensure that information is accurate, up-to-date and complete.

An individual can also make a complaint to the Information Commissioner and the complaint may related to a serious credit infringement. The Commissioner would be able to exercise the full range of powers in relation to any such complaint. After investigating, the Commissioner may also make a determination in relation to that investigation.

The Department is not able to express a view on whether a credit provider should list a serious credit infringement in circumstances where an individual has suffered the consequences of a natural disaster. However, the Department notes that the definition of serious credit infringement requires the credit provider to be satisfied that a reasonable person would consider the individual's act (for example, of missing one or more payments because of a natural disaster) indicates an intention to no longer comply with the individual's obligations.

Consumer credit variations on the grounds of hardship

The Bill does not deal with consumer credit variations on the grounds of hardship. This means that a hardship variation cannot be included in an individual's credit reporting information.

The right of an individual to request a hardship variation in relation to consumer credit obligations is set out in section 72 of the National Consumer Credit Protection Act 2009, which says:

> (1) A debtor who is unable reasonably, because of illness, unemployment or other reasonable cause, to meet the debtor's obligations under a credit contract and who reasonably expects to be able to discharge the debtor's obligations if the terms of the contract were changed in a manner set out in subsection (2) may apply to the credit provider for such a change.

Subsection (2) lists certain changes that may be sought, including extending the period of the contract, reducing payments, or postponing payments for a specified period.

Credit reporting industry representatives have argued that a 'hardship flag' should be available for inclusion in the credit information of an individual who has been provided with a hardship variation. The Government has not accepted that listing of hardship variations is a necessary component of the credit reporting system. The Government accepted ALRC recommendation 58-2 to include new arrangement information (defined in clause 6S) as part of an individual's credit information. However, new arrangement information only refers to an arrangement made after a person has defaulted or committed a serious credit infringement. New arrangement information is not the same as a hardship variation. An individual can request a hardship variation before the individual defaults or commit a serious credit infringement. The Department notes that submissions from consumer credit advocates (for example, the Consumer Action Law Centre, submission 5, page 1) are opposed to any approach to listing hardship variations that may discourage consumers from requesting hardship variations.