Attorney-General's Department – response to House Standing Committee on Social Policy and Legal Affairs questions on notice provided 16 August 2012

Question 1 - direct marketing

Many submissions (ADMA, Foxtel, Salmat) suggest that the direct marketing section of the Bill is entirely misleading in its suggestion that there is a prohibition on direct marketing because the numerous permit it in many circumstances. This may be misleading not only to consumers but also to advertising organisations.

(a) Is there a logical reason for drafting the section in this way?

(b) Is the LCA's concern that this reverses the burden of proof a valid one?

Departmental response

(a) 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.

(b) The LCA asserts that certain provisions have the effect of reversing the onus of proof because of the drafting approach in certain provisions that prohibit activity with specific exceptions. For example, clause 20C prohibits the collection of solicited credit information except in specified circumstances. The LCA submits that this reverse burden in clause 20C is difficult to bear and may lead to decreased competition and risk aversion in the credit reporting industry.

As noted above, the most effective drafting approach for privacy regulation is 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. It is consistent with the approach taken in the existing Act and with other provisions in the Bill, including those relating to credit reporting which the LCA has raised issues about (eg clause 20C).

The concept of placing a burden on an entity to prove certain matters – which is more familiar to evidential burdens in court cases – is not an accurate description of the practical operation of the provisions in the Bill. The obligation on entities that wish to undertake the activity that is not permitted is to handle the information concerned in accordance with the exceptions. In the event of an investigation by the OAIC, the Privacy Commissioner will consider whether the entity has breached the provision by not coming within the exceptions. In cooperating with an investigation, there is no presumption that the entity has to rebut.

The LCA's concerns appear to centre more around the difficulty that credit reporting bodies (CRBs) may have in complying with clause 20C. The Department does not believe that the requirements that CRBs need to meet to fall under the clause 20C exceptions are too severe. CRBs will be expected to ensure that credit information entering the credit reporting system has, among other things, an Australian link and does not relate to minors. The credit information held by CRBs can have significant impacts on individuals, which is why privacy protections are so important in this field. Under the amendments, more information will be allowed to be used in the credit reporting system, and it is therefore important that there are appropriate privacy protections for consumers around this new information.

Question 2 - 'opt out' options for direct marketing

Advertising industry representatives (Foxtel, ADMA, joint social media submission) suggest that the requirement to provide an 'opt out' option is highly impractical in media such as twitter or facebook. Is this an unreasonable requirement in such circumstances?

Departmental response

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 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. 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.

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.

Question 3 - reasonably necessary

The ALRC and OAIC query the standard shift of 'reasonable necessary' in the Bill. The EM suggests that 'reasonably necessary' is intended to be interpreted in an objective way and is not intended to provide a lower level of privacy protection than the NPPs (which had a standard of 'necessary'). On this basis, the OAIC suggests that the distinction between 'necessary' and 'reasonably necessary' is arbitrary and confusing. The distinction may therefore be arbitrary but it also appears to have the potential to compromise privacy protection in some situations. Do you consider that the circumstances in which the 'reasonably necessary' standard is included can always be adequately justified?

Departmental response

The Department believes that the inclusion of a 'reasonably necessary' standard in each circumstance in which it appears in the Bill is justified.

First, the concepts of 'reasonably necessary' and 'necessary' coexist in the existing Privacy Act without any confusion or compromise on privacy protection. For example, the 'reasonably necessary' formulation currently appears in both the NPPs and the IPPs in relation to exceptions for law enforcement activity (see, for example, IPP 10.1(d) and NPP 2.1(h)). As with the existing approach taken in the Bill, this is to provide additional certainty that an objective test applies in these circumstances.

Further, the existing Privacy Act recognises that there are instances where an objective element applies to an activity where the 'necessary' formulation appears. For example, NPP 2.1(e) provides that the use or disclosure of personal information for a secondary purpose may occur where an organisation 'reasonably believes' that it is 'necessary to lessen or prevent a serious and imminent threat' etc. A similar approach is taken with the corresponding exceptions in IPP 10.1(b) and 11.1(c). That is, it is not necessary to include a 'reasonably necessary' formulation because an objective element has already been included to target another aspect of the activity (ie the entity's belief at the time).

The general approach taken in the Bill reinforces this current approach from the Act. First, the 'reasonably necessary' formulation is used in APPs 3, 6, 7 and 8, and exceptions listed in clause 16A, to provide clarity that an objective test applies in relation to each of those activities. Secondly, where the 'necessary' formulation is used on its own, the addition of 'reasonably' is not required because it preceded by a 'reasonably believes' test (see, for example, items 1, 2, 3, 6, and 7 in table in clause 16A).

In relation to enforcement body and enforcement related activity exceptions, a dual 'reasonably believes' and 'reasonably necessary test applies, but that it based on the operation of the existing NPP 2.1(h). In 'Information Sheet (Private Sector) 7 - 2001: Unlawful Activity and Law Enforcement', the Office of the Australian Information Commissioner provides the following guidance about this provision:

> A 'reasonable belief' is a belief that might reasonably arise in the circumstances based on the facts of the situation. A use or disclosure might be considered 'reasonably necessary' if an enforcement body cannot effectively carry out its functions (as specified in NPP 2.1(h)(i) to (v)) without the organisation using or disclosing personal information.

The two pronged objective test in this provision (ie relating to an organisation's belief, and the necessity of the use or disclosure) is an additional safeguard to guard against inappropriate use or disclosure by a private sector organisation for a law enforcement purpose. It has been working effectively to date and is therefore being retained in the APPs using the same terminology (see, for example, APP 3.4(d), APP 6.2(e) and APP 8.2(f)).

Question 4 – complexity

Numerous submissions state that the Bill is overly complex and inaccessible.

(a) Are you considering any redrafting or restructure of the Bill to remedy this?

(b) Are you or the OAIC planning to develop any educational materials to accompany the new privacy regime?

Departmental response

(a) The Department is not considering any comprehensive redrafting or restructuring of the Bill. The Government agreed with recommendation 2 of the Senate Finance and Public Administration Legislation Committee Report on the Credit Reporting Exposure Draft and the Department reviewed the drafting and structure of the provisions during the preparation of the Privacy Amendment Bill.

Stakeholders may feel the Privacy Amendment Bill introduces greater length and complexity. As an amendment Bill, the structure of some of the reforms may not be readily discernible but it is expected the structure will become apparent when the amendments are incorporated into the Privacy Act as a single document. In addition, the Privacy Amendment Bill implements 111 of the ALRC recommendations for legislative action addressed in the Government's first stage response, while preserving unchanged many existing policy matters. In relation to credit reporting, the Department notes that the credit reporting industry appears to have significantly increased in complexity and scale since the credit reporting provisions were introduced over 20 years ago. The credit reporting provisions deal with what the Department understands are the actual information flows currently occurring in the credit reporting system, at the same time introducing modifications (such as the introduction of more comprehensive credit reporting) recommended by the ALRC. Our understanding of the information flows in the credit reporting system, and the need to use specific terms to aid reference to elements of those information flows, is discussed in detail in the Explanatory Memorandum at pages 93 to 100.

(b) The ALRC made numerous recommendations directed to the Office of the Privacy Commissioner (now the OAIC) for the provision of guidance and education material. The Government accepted these recommendations in principle and supports the development of educational materials consistent with the OAIC's function of providing guidance (which has been revised and is now set out in clause 28, schedule 4 of the Privacy Amendment Bill). The development and promulgation of education and other guidance materials is a matter for the Commissioner.

Question 5 - Australian link

Many submissions suggest that the 'Australian link' requirement is unreasonably restrictive. There are proposals that instead, APP8 should apply to credit reporting information in the same way it applies to personal information (ARCA, ABA, GE, Telstra). How are you planning to resolve the issues around the Australian link requirement?

Departmental response

The Privacy Act has specifically regulated credit reporting in Australia since Part IIIA was inserted into the Act in 1990. The amendments were announced by the then Government in May 1989 following public controversy over the credit industry's intention to introduce a system of routine monitoring of consumer credit. Credit reporting involves significant personal financial data. The credit reporting provisions have always been concerned to

ensure that an appropriate balance is maintained between the interests of credit providers in having access to sufficient personal information to assess credit worthiness and the interests of individuals in the protection of their personal information.

The Government accepted ALRC recommendation 54-5 to exclude the reporting of personal information about foreign credit and the disclosure of credit reporting information to foreign credit providers. There was no policy intention to prohibit the existing practices of credit providers in relation to off-shore processing of personal information in the credit reporting system. The off-shore processing of credit reporting information does not appear to have been considered by the ALRC.

The term 'Australian link' has been used to limit collection, use and disclosure of personal information in the credit reporting system. On examining the exposure draft of the credit reporting provisions in the development of the Privacy Amendment Bill, it became clear that permitting broad cross-border disclosure of personal information from the credit reporting system under APP 8 would undermine the Government's policy to exclude the reporting of personal information about foreign credit and the disclosure of credit reporting information to foreign credit providers.

While the term 'Australian link' has not previously been used in the credit reporting provisions, it is an existing term in the Privacy Act. The term 'Australian link' is used in section 5B in relation to the extra-territorial operation of the Act to ensure that the Act cannot be avoided by simply holding information outside Australia.

Subsections 5B(2) and (3) define the term 'Australian link' to describe the kind of link that an organisation must have with Australia. Subsection 5B(2) will, as amended, state that an organisation or small business operator must be:

a) an Australian citizen; or

b) a person whose continued presence in Australia is not subject to a time limitation imposed by law; or

c) a partnership formed in Australia or an external Territory; or

d) a trust created in Australia or an external Territory; or

e) a body corporate incorporated in Australia or an external Territory; or

f) an unincorporated association that has its central management and control in Australia or an external Territory.

Subsection 5B(3), as amended, extends the definition of 'Australian link' to certain other situations. This extended definition applies when all the following conditions are satisfied:

a) the organisation or operator is not described in subsection (2);

b) the organisation or operator carries on business in Australia or an external Territory; and

c) the personal information was collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice.

The term 'Australian link' is used in the credit reporting provisions to provide an effective limitation on the collection, use or disclosure of personal information in the credit reporting system. For example, clause 20F(1)(a) provides that a credit reporting body can only disclose credit reporting information to an entity that has an Australian link (and the other specific conditions set out in the table must also be satisfied). This restriction protects the personal

information of individuals by ensuring that their information is only disclosed to entities that are subject to the obligations of the credit reporting provisions.

The Department's view when inserting the term 'Australian link' into the credit reporting provisions was that the extended meaning of 'Australian link' in subsection 5B(3) (which includes a foreign organisation or operator that is not otherwise based in Australia but which collects or holds information in Australia), in conjunction with the permission for credit providers to disclose to a related body corporate, would be sufficient to allow off-shore processing while ensuring that consumers were protected under the credit reporting provisions.

Credit provider stakeholders have expressed the view that the provisions would not be sufficient to allow them to continue to undertake off-shore processing of credit reporting information.

The Department is considering options to address this issue. The structure of the credit reporting provisions is to prohibit all collection, use and disclosure of personal information in the credit reporting system and then provide targeted exceptions for permitted acts and practices. As noted above, the Department considers that simply applying APP 8 without any modification may undermine the policy of not disclosing Australian credit information to foreign credit providers. The Department's preferred approach is to identify options to provide specifically for a targeted disclosure (and associated use) to deal with off-shore processing. Such a targeted provision could then impose obligations based on APP 8.1 and proposed section 16C of the Privacy Amendment Bill to ensure that the Australian credit provider remains accountable for the personal information in the hands of the overseas processor recipient. Initial discussions with credit provider stakeholders indicate that this approach may be acceptable to them. We will continue to work with stakeholders to refine an approach that can be put to the Attorney-General for consideration.

Question 6 - repayment history

The Consumer Credit Legal Centre suggests that including repayment history as the fifth data set in the credit reporting scheme may lead to risk-based pricing, will entrench hardship and will leave consumers worse off with credit becoming extremely expensive. CCLC claims this will leave disadvantaged consumers most detrimentally affected (senate hearing transcript, page 30). Do you agree that this may be the effect and have you considered introducing any measures to address these concerns?

Departmental response

The ALRC considered the arguments for and against the inclusion of repayment history information in the credit reporting system. ALRC recommendations 55-2 to 55-5 said that, on balance, limited repayment history information should be included, subject to the introduction of responsible lending obligations and other safeguards for consumers.

Repayment history information is one of a number of new types of personal information that will be permitted in the credit reporting system as part of the Government's move to a more comprehensive credit reporting system. The other types of personal information will be: the type of consumer credit; the date a consumer credit account is entered, or the date on which it is terminated; and the maximum amount of credit available under the consumer credit. The Government considers that more comprehensive credit reporting will allow more robust assessment of credit risk, which in time could lead to lower credit default rates. The Government considers that, on balance, more comprehensive credit reporting is likely to

improve competition in the credit market, which will result in benefits to both individuals and the credit industry.

The risks and benefits of the inclusion of repayment history information were considered in the Regulation Impact Statement (set out in the Explanatory Memorandum for the Privacy Amendment Bill). The RIS identified a number of potential risks and benefits for individuals, credit reporting agencies, credit providers, and small businesses (pp25 to 27 of the Explanatory Memorandum). The conclusion was that, on balance, repayment history information should be included in the credit reporting system (p29 of the Explanatory Memorandum). The Government considered the RIS in determining that limited repayment history information should be included in the credit reporting system.

Industry stakeholders have provided submissions supporting the introduction of repayment history information. There is no agreed stakeholder position on the likely implications of including repayment history information. The Department does not consider that any additional legislative measures in the Privacy Amendment Bill would resolve the disagreement between stakeholders on the possible implications of including repayment history information in the credit reporting system.

The consumer protections recommended by the ALRC around repayment history information have been included in the Privacy Amendment Bill. These include:

- A restrictive definition of 'repayment history' in section 6V
    - in addition, regulations will be made to provide further guidance on the elements of the definition
    - stakeholder consultation on the content of the regulations has commenced
    - matters such as a 'grace period' before reporting can be considered by stakeholders and included in the regulations or CR code if there is agreement
- Strong restrictions on the collection, use and disclosure of repayment history information
    - CRBs can only disclose to credit providers that are subject to responsible lending obligations - subclause 20E(4)
    - CPs can only disclose repayment history information to a CRB as part of credit information if the CP is a licensee – paragraph 21D(3)(c)
    - CPs cannot disclose credit eligibility information that includes repayment history information unless the disclosure complies with specific requirements - subclauses 21G(4) and (5)
- Repayment history information cannot be used for pre-screening – paragraph 20G(2)(c)
- CRBs are only permitted to retain repayment history information for 2 years – clause 20W item 2 (and any information derived from the repayment history information is subject to the same limited retention period of 2 years – subclause 20V(5)).

The Government accepted ALRC recommendation 54-8 proposing a review of the credit reporting provisions. The Government response stated that a review of the credit reporting provisions would be conducted within 5 years from the commencement of the provisions.

The review will provide an opportunity to consider evidence on the use of repayment history information in the credit reporting system.

Question 7 - addresses stored on file

Veda's submission suggests that the proposed approach to address storage should be altered to include either current address plus two previous or all addresses within the last 5 years, whichever the greater, as many individuals will become untraceable under the proposed system (Veda suggested approximately 300,000 individuals at page 23 of the senate hearing transcript). What is your view on such an amendment?

Departmental response

Address information is used as one of a number of types of personal information to identify an individual and ensure they are appropriately linked to personal information in the credit reporting system. The types of personal information that are currently permitted to be used as identification information are set out in the current OAIC Credit Reporting Determination 1991 no. 2 concerning the identifying particulars permitted to be included in a credit information file. The then Commissioner considered a range of personal information that was proposed as identifying information. In relation to address information the Commissioner found that an individual's current address, plus two previous addresses (if any in the preceding five year period), could be retained as identifying information for an individual. In this regard the Commissioner provided the following reasons:

> *Previous addresses*: In the light of consultation with credit reporting agencies and the long experience of the New South Wales Privacy Committee in this field, I am satisfied that there is a need for a credit reporting agency to keep an individual's previous address information to assist in ensuring that an enquiry from a credit provider who might, for example, have an old address, is properly matched. In the interests of privacy, reasonable limits should be placed on the possibility of a history of addresses being compiled. Accordingly, this category of information on the file should be limited to only two immediately previous addresses. (Credit Reporting Determination 1991 no. 2, paragraph 5(ii), available at http://www.privacy.gov.au/index.php?option=com_icedoc&view=types&element=determinations&fullsummary=6874&Itemid=1021)

The definition of 'identification information' to be inserted into subsection 6(1) by item 34 of schedule 2 of the Privacy Bill is directly based on OAIC Credit Reporting Determination 1991 No.2. 'Identification information' is included as one of the permitted types of personal information included in the definition of 'credit information' in section 6N of the Amendment Bill. In setting out an exhaustive list of the types of personal information that are permitted to be included in the credit reporting system, the Government is implementing ALRC recommendation 56-1. The ALRC did not recommend any changes to the types of identifying information that should be permitted. The ALRC does not appear to have identified or discussed the risk that the current limit on the number of previous addresses included in the credit reporting system may increase the possibility that a significant number of individuals may become untraceable.

The Department does not consider that credit reporting bodies will lose all information about an individual if the individual moves more than twice in five year period. This is not the Department's understanding of the effect of the definition of 'identification information' or the proposed operation of the credit reporting provisions. The Department notes that the proposed definition of 'identification information' includes a range of other types of personal

information, including the individual's current or last known employer and the individual's driver's licence number (if they hold a licence). A credit reporting body will need to update address information about any individual who moves, whether the individual moves once or many times in a five year period. Address information is available to ensure accurate identification of the individual when considered in conjunction with the range of other identification information available under the definition.

The Department considers that the various types of personal information included in the definition of 'identification information', in conjunction with the permitted address information, should be sufficient to identify individuals. In forming this view the Department has consulted with the OAIC, which is satisfied that the proposed definition of 'identification information' is consistent with the current OAIC Determination and remains sufficient for identification purposes.

Question 8 - depersonalised data

Veda's submission notes that the ALRC did not recommend any provisions on depersonalised data and that no other modern economy includes provisions on depersonalised data in their privacy laws. Several groups have called for s 20M to be removed from the Bill in its entirety and suggest that, not being personal information, it should not be regulated by privacy laws. We understand that some exceptions exist in relation to the use of depersonalised data but given the importance of the work it produces and the fact that it isn't regulated elsewhere in the world, why did you decide to regulate it in the Bill at all?

Departmental response

The Government supports the use of de-identified credit reporting information for research purposes in relation to the assessment of credit worthiness of individuals. The purpose of clause 20M is to ensure that the Information Commissioner has the power to issue appropriate guidelines to deal with how an individual's personal financial information may be used for research.

The use of personal information for research is a secondary use. The Government response to ALRC rec 57-2 stated that secondary uses would not be permitted for unknown purposes. The Government response specifically identified research as a use that should be permitted. Credit reporting agencies had previously advised the ALRC that they 'removed' credit reporting information from the credit reporting system. This was noted in the ALRC report at paragraph 58.116, which says that Veda argued credit reporting agencies:

> should be able to 'continue to hold credit reporting information for the building of statistical models' beyond the retention periods prescribed . . . Veda advised that this is currently done by removing the information from an individual's 'credit information file', as that term is defined in the Act.

The use of personal information for statistical modelling appears to be a significant component of the research done by credit reporting agencies. Credit reporting agencies subsequently advised that they de-identify personal information before using it for research purposes. However, it was unclear how de-identification was done and whether this included removal from the credit reporting system. The Government's view was that research was an appropriate secondary use but, given the uncertainty at the time around whether and how the personal information was de-identified, the best approach was to expressly permit the use of de-identified credit reporting information for research purposes subject to certain conditions.

Credit reporting bodies are permitted to use de-identified information for conducting research in relation to the assessment of the credit worthiness of individuals. In addition, the research must comply with OAIC rules. A similar provision was included in the credit reporting exposure draft. Credit reporting agencies have not previously provided information on the full nature and scope of the research they currently conduct with personal information from the credit reporting system. However, any current research that can be considered to be in relation to the assessment of the credit worthiness of individuals would be permitted to continue, once the OAIC has prepared the necessary rules to provide general guidance on this research.

Question 9 - transition period

Many industry submissions (ABA, Veda, AFC) suggest the 9 month proposed transition period from royal assent to commencement is unreasonable and won't allow industry to establish internal systems to deal with new obligations- a process that cannot be undertaken until the CR code is finalised. The Australian Finance Conference suggests that the Bill should include a provision allowing the Attorney-General to nominate a revised commencement date if required. Is this an approach you are considering?

Departmental response

The Department proposed an extension to the standard three month period between Royal Assent and commencement of the Bill to provide sufficient time for the development, approval and registration of the Credit Reporting Code. The CR Code is an essential part of the regulatory structure of the credit reporting provisions, providing practical guidance for stakeholders on the operation of the credit reporting provisions. The Department considered, based on advice received from the OAIC, that a 9 month commencement period would be a sufficient period leading to registration of the CR Code.

The Department considered the commencement periods provided for the introduction of other relevant regulatory changes in proposing the 9 month commencement period. The introduction of the private sector privacy reforms in 2000 was subject to a 12 month commencement period. The NCCP Act reforms had a two year implementation period. The FOI Act reforms commenced by proclamation after 5 months, but were subject to a default commencement period of 6 months. In proposing a 9 month commencement period the Department was also aware of strong credit reporting stakeholder concerns that the reforms should not be delayed.

We note that stakeholder submissions have expressed a range of views on an appropriate commencement period. Stakeholders have variously suggested: extending the commencement period to 12 or 18 months or even two years; implementing the privacy reforms in stages, including by providing a 'grace period' during which the OAIC would focus on education and the development of compliance procedures in organisations; and providing for commencement at a time to be nominated by the Attorney-General only if certain actions (the registration of the Credit Reporting Code) have been completed.

The Department considers that the commencement period should provide sufficient time for the development, approval and registration of the CR Code, provide certainty by setting out a defined time in the legislation for commencement, and should see all elements of the Privacy Amendment Bill commence at the same time (that is, no staged implementation). The Department does not consider that commencement should be at the discretion of the Attorney-General, nor does the Department consider that commencement should be contingent on the registration of the CR Code as this does not ensure certainty. The

Department will be considering stakeholder views on extending the current proposed 9 month commencement period in proposing options for the Attorney-General's consideration.

Question 10 - requirement for Commissioner to make a determination

The Bill allows the Privacy Commissioner to make a determination in relation to a dispute, and that determination can be appealed at the AAT. However, the Australian Privacy Foundation's submission notes that given the Privacy Commissioner's perceived reluctance to make determinations, this right is meaningless without the inclusion of an obligation on the Commissioner to make a determination where an individual or entity requests that he do so. Did you consider including such an obligation in the Bill? Why/why not?

Departmental response

Determinations

The small number of determinations does not necessarily indicate that the Privacy Commissioner has been reluctant to make determinations. Under the Act, the Commissioner is required to attempt to conciliate privacy complaints before initiating more formal processes. Individuals making complaints are often seeking informal and above all *private* outcomes. The small number of determinations suggests that the Commissioner's conciliatory approach has been successful. The Department is not aware of any evidence of widespread dissatisfaction with the way in which the Commissioner has resolved complaints through the conciliation process.

It should also be noted that a decision by the Commissioner not to make a determination is subject to judicial review. Complainants unhappy with the Commissioner's decision not to make a determination may apply to the Federal Court or Federal Magistrates Court under section 5 of the *Administrative Decisions (Judicial Review) Act 1977* for a review of that decision.

Compliance-oriented regulatory design

The Department agrees that determinations by the Commissioner may be of assistance to lawyers and members of the public in interpreting the Act. However, the Commissioner already assists in the interpretation of the Act in a number of other ways. For example, the Commissioner has published a number of fact sheets and guidelines that clarify privacy rights and obligations under the Act.

Privacy complaints often relate not only to interference with an individual's privacy but also to systemic issues relating to the ways in which agencies and organisations handle personal information. Adversarial proceedings are not the most effective way to resolve this kind of systemic and cultural issue. This is reflected in the ALRC's recommendations regarding the powers and functions of the Privacy Commissioner. The ALRC adopted the notion of an outcomes-based or 'compliance-oriented' approach to regulation, in which all the factors of regulatory rule making, monitoring and enforcement are designed to elicit a particular regulatory objective. With its focus on achieving outcomes, the ALRC considered that compliance-oriented regulation provided a useful framework to administer a principles-based regime such as the Act.

The ALRC grouped the elements of compliance-oriented regulation under three concepts:

- securing or fostering voluntary compliance with the regulatory objectives
- undertaking informed monitoring for non-compliance, and

- engaging in enforcement actions where voluntary compliance fails.

In relation to the third element, the ALRC considered that in a compliance-oriented regulatory design, a regulator's response to non-compliance in a principles-based regime can be characterised as rehabilitative, rather than punitive. However, to be effective, attempts to nurture and restore compliance must operate in the presence of more punitive sanctions. The ALRC referred to this approach as an 'enforcement pyramid' approach, where a regulator can start with persuasive or restorative strategies and then move to more punitive strategies if voluntary compliance fails. Self-regulation and co-regulation also form part of the enforcement pyramid model.

The Bill consolidates and redrafts the provisions dealing with the functions and powers of the Commissioner. The structure of the new sections will follow a compliance-oriented approach to regulatory design. The Commissioner's functions will be grouped according to whether they foster compliance (the guidance related functions), monitor compliance (the monitoring related functions) or support compliance (the advice related functions). The Commissioner's exercise of these functions is expected to reduce the number of privacy complaints and hence the need for determinations. For example, the Commissioner's guidance related functions include making guidelines for the avoidance of acts or practices that may or might be interferences with privacy of individuals, or which may otherwise have adverse effects on the privacy of individuals.

The Bill also provides—in response to ALRC Recommendation 47-6—that the Commissioner may conduct an assessment of an agency's or organisation's maintenance of personal information. This discretion will allow the Commissioner to take a snapshot of the compliance levels in an agency or organisation or across an industry. Spot assessments can act as an important preventative measure by encouraging entities to take compliance with the Act seriously. The assessments are intended to be of an educational and non-confrontational nature, and to provide an avenue for the Commissioner to give one-on-one guidance to an entity without needing to resort to mandatory enforcement action.

Merits review

Clause 96 provides for merits review by the AAT of a number of decisions by the Commissioner, including a decision under subclauses 52(1) or (1A) to make a determination. Clause 96 implements ALRC Recommendation 49-7 by expanding the availability of merits review by the AAT of determinations made by the Commissioner. Increasing the availability of merits review is intended to promote further transparency and accountability in the Commissioner's decisions. However, expanding merits review to decisions by the Commissioner not to make a determination, or including a right of complainants to require the Commissioner to make a determination, would be at odds with the compliance-oriented regulatory design recommended by the ALRC.

Question 11 - exceptions/defences to liability for disclosure

There is significant concern that entities remain liable for information breaches beyond their control. Many organisations are concerned that once transferring information overseas, the disclosing Australian company remains liable for a breach that is beyond their control. Australian Bankers Association's submission suggests that an exception should exist to the civil penalty where the disclosure was inadvertent and the entity acted honestly and reasonably. Alternatively, Salmat's submission suggests that a breach should only exist where the disclosure was reckless or intentional. Did you consider such exceptions/defences in relation to the civil penalty provision in this Bill?

Departmental response

In developing APP 8 the Government decided that a new policy approach to cross-border disclosures of personal information was necessary. The accountability approach in APP 8 will ensure effective cross-border protection for the personal information for individuals and is consistent with both OECD and APEC privacy developments. APP 8 ensures that individuals whose information is disclosed to an overseas recipient continue to have an Australian entity that is responsible for the protection of their personal information.

APP 8 balances the commercial and other interests of entities in making cross-border disclosures with the interests of individuals in effective privacy protection. In place of the existing prohibition in NPP 9, an entity is generally permitted to make a cross-border disclosure of personal information. However, before making any cross-border disclosure the entity must take such steps as are reasonable in the circumstances to ensure the overseas recipient does not breach the APPs. This is the statement of the accountability approach – an entity is generally permitted to make cross-border disclosures, but remains accountable for the acts and practices of the recipient in relation to any personal information that is disclosed. This provision is supported by additional notice requirements to individuals around cross-border disclosures.

The Government considered that APP 8.1 should not include any general exceptions as this would undermine the confidence of individuals in the protection of their personal information. Similarly, section 16C (which ensures that entities are responsible for the acts and practices of overseas recipients) does not contain any exceptions or defences. The only exceptions permitted are those set out in APP 8.2. The exceptions in APP 8.2 have been carefully considered and the Government considers that they are justified. The Government considers that these exceptions provide appropriate and reasonable grounds for the transfer of accountability to an overseas recipient. In all other situations, the Australian entity should continue to remain accountable for the protection of personal information.

The Government does not consider that an exception is necessary where the overseas recipient may have made an inadvertent disclosure of personal information. An inadvertent disclosure of personal information by an overseas recipient may have significant consequences for an individual. While a disclosure may be inadvertent, the fact the disclosure has occurred may indicate failures in the security systems or handling protocols of that personal information in the hands of the overseas recipient. These are matters that can be taken into account in an OAIC determination, or by a court if the matter was being considered in relation to a possible civil penalty for the Australian entity. It is not automatically the case that all possible or actual breaches of APP 8.1 will result in the imposition of a civil penalty. The decision to obtain a civil penalty order is at the discretion of the Commissioner, while the decision on whether a civil penalty should be imposed is at the discretion of the court.

The Government does not consider that an exception is necessary to deal with situations were an overseas recipient has recklessly or intentionally performed an act or practice that has led to a breach of an individual's personal information. In such circumstances, the overseas recipient may not be readily subject to the jurisdiction of the OAIC or an Australian court. Again, while the actions of an overseas recipient may be taken into account in an OAIC determination or by a court if the matter was being considered in relation to a possible civil penalty for the Australian entity, the Government does not consider that this is sufficient reason to transfer accountability to the foreign recipient. The circumstances in which accountability can be transferred to a foreign recipient are set out in APP 8.2.