AUSTRALIAN BANKERS' ASSOCIATION INC.

Steven Münchenberg
Chief Executive Officer

AUSTRALIAN BANKERS' ASSOCIATION INC.
Level 3, 56 Pitt Street, Sydney NSW 2000
p. +61 (0)2 8298 0401 **f.** +61 (0)2 8298 0402

www.bankers.asn.a

16 July 2012

Ms Julie Dennett
Committee Secretary
Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
CANBERRA ACT 2600

Email: legcon.sen@aph.gov.au

Dear Ms Dennett,

Privacy Amendment (Enhancing Privacy Protection) Bill 2012

The Australian Bankers' Association (ABA) appreciates the extension of time granted by your office for lodging this submission.

The Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Bill) that includes the single national Australian Privacy Principles (APPs) with the addition of a more comprehensive credit reporting regime are welcome and timely developments towards a more seamless and nationally focused Australian privacy regime. The ABA compliments the Government on its leadership and commitment in initiating these reforms.

The ABA is the peak national body representing 26 member banks that are authorised by the Australian Prudential Regulation Authority (APRA) to carry on banking business in Australia. Members of the ABA include the four major Australian banks, foreign banks that are represented and carry on banking business in Australia as Australian banks and former regional banks that now operate nationally.

Member banks operate on a national scale and many have international relationships and interfaces. Some banks also have contractual arrangements with certain Commonwealth and State agencies.

The ABA's involvement with the national privacy regime dates back to the 1990s when it participated on the then Privacy Commissioner's consultative group that developed the National Principles for the Fair Handling of Personal Information, the forerunner to the National Privacy Principles (NPPs) that underpin the private sector provisions of the Privacy Act today.

In 2010 the ABA provided a submission to the Senate Finance and Public Administration Committee on the Exposure Draft of the Australian Privacy Principles and Companion Guide and a later submission to that Committee in March 2011 on the Exposure Draft Australian Privacy Amendment Legislation - Credit Reporting Bill.

The ABA appreciates the opportunity provided by your Committee to submit its views on the proposed privacy reforms in the Bill, in particular, on the APPs.

Submission outline

In outline, this submission provides -

1. An introduction.
2. An explanation of the respective roles of the ABA and the Australasian Retail Credit Association (ARCA) regarding the credit reporting and other privacy provisions in the Bill.
3. A concern that the proposed commencement date is premature.
4. Substantive submissions on some definitions, in particular the definitions of "Australian law" and the effect of the definition of "Australian link", the APPs, complaints handling, enforcement, and the need for transitional provisions.

1. Introduction

Privacy is not a new concept for banks. For almost 150 years the courts have recognised that a bank owes a duty of confidentiality to its customers. This has become an implied term in every contract for banking services between a bank and its customer.[1]

The duty of confidentiality is a duty by a bank not to disclose its customer's affairs unless certain exceptions apply. This duty has survived the Privacy Act and continues to be observed today.

Personal information that is collected by a bank comes from a wide variety of sources in connection with the management of the bank and the customer relationship under the law and applicable codes of conduct. Typically, a bank will have millions of customers with an even greater number of customer account relationships. Sources of personal information relevant to its customers received by a bank include conversations with customers in branches, over the telephone and in call centres, by email, ordinary mail and from transactions payments systems, bodies such as clearing houses and card schemes. More recently, there is a trend where customers are preferring for information to be exchanged between the bank and customer through what are generally described as social media, for example on Twitter and Facebook.

A bank will have subsidiaries that provide additional financial services to complement the bank and its customer relationship such as with general insurance and financial advisory and investment services where some personal information sharing between these entities is necessary in order to meet customers' needs.

A bank's ability to identify the sources and monitor the collection of personal information and to be able to share this information appropriately within its own banking group in conformity with privacy and other financial services regulation, is a significant and complex task. The objective is to ensure the best seamless relationship experience for the customer consistent with the customer's expectations and for compliance with privacy and other laws that apply to banking and financial services activities.

---

[1] See Foster v Bank of London (1862) 176 ER 96. The leading case is Tournier v National Provincial and Union Bank of England [1924] 1KB 461

2. Roles of the ABA and ARCA

As ARCA's submission to the Committee will describe, ARCA is the peak body representing financiers and other participants in the wider credit industry concerned with credit reporting activities. ARCA's membership includes a number of the ABA's members.

To avoid duplication and overlap, ARCA is making submissions on behalf of its members regarding the credit reporting provisions in Schedule 2 of the Bill and any other associated issues in other Schedules of the Bill.

Some members of the ABA may choose to make their own submissions to the Committee which the ABA is pleased to support.

The ABA supports ARCA's submissions and individual ABA member submissions. The ABA confines its submissions to the non-credit reporting aspects of the Bill other than any credit reporting issues that are not covered in ARCA's submission or about which the ABA wishes add emphasis and its support.

3. Commencement date

The proposed commencement date in the Bill is 9 months following Royal Assent to the Bill.

Implementation of the reforms associated with the APPs could require a different timeframe to those reforms relating to Part IIIA of the Act. With the former, implementation is primarily an exercise for individual banks to undertake. The credit reporting reforms will require individual banks to develop their own internal compliance arrangements together with ensuring that their IT systems can interface with external credit reporting bureaux systems. Further, credit reporting bureaux will have to implement their own compliance arrangements.

These dependencies have timing implications including the development of the revised Credit Reporting Code of Conduct that must be approved by the Privacy Commissioner after required consultation arrangements have been completed. These aspects require particular consideration which ARCA is addressing in its submission.

The ABA considers that as far as the general privacy provisions are concerned, the proposed implementation timeframe in the Bill will be insufficient for our members to implement those reforms effectively.

For banks, major practical considerations for implementation of regulatory reform are staff training, documentation and IT system changes. Proper implementation of regulatory reforms is a serious matter. Non-compliance can often mean civil or criminal penalties for staff and/or for the bank, liability to pay compensation, costly reworks or manual workarounds if the implementation timeframe is too short and damage to a bank's reputation. Non-compliance with the law could also disrupt the normal course of business for bank customers.

In relation to staff training, a large retail bank typically will have thousands of frontline staff in addition to back office and support staff who may also need to be trained. This training requires a detailed change management plan that takes account of the impacts to different service delivery channels (for example branch, call centre, on-line, mobile bankers and so on). Training techniques for those different staff need to be targeted so that they understand the changes and the resulting changes to their processes, policies and procedures and what is to be expected of them.

The design phase of in-house training can only commence once the legislative requirements (primary and subordinate) have been finalised. This may include any supplementary regulatory instruments or

guidance issued by relevant regulators. The design phase can take some months if the changes are complex.

In relation to IT system changes, there are only a limited number of changes a bank may make every year to its IT environments. This is driven primarily by internal competition for resources. Exceeding this threshold increases the risk of change driven IT systems failures that may directly impact the bank's customers. In order to accommodate a compliance and regulatory related project, a bank may have to scale back its normal business projects that add value to the bank's customers, such as improving services or introducing new products, in favour of regulatory compliance changes.

To manage risk, portfolio planning is generally undertaken a year in advance. Defining the requirements for all systems impacted (this can be between 30 to 40 systems for a large conglomerate group) can take between three to six months depending on the number of systems impacted by the changes. Systems for integrating the engagement by the bank with external parties such as brokers and other financial intermediaries need to be taken into consideration.

During anticipated peak processing periods such as end of financial year and end of the calendar year a bank will implement change freezes for IT related changes. Any regulatory changes that come into effect around those times (July and January) will further add to the complexity of having to implement, test and be ready ahead of the IT change freeze timeframes. These dates are also challenging for staff training given the higher than usual absences around Christmas/New Year and higher than usual workloads to assist customers with end of financial year inquiries. As a result, staff training may have to occur well in advance of the actual launch date, which can lead to difficulties with ensuring that the training is complete and effective and reaches all staff employed in affected roles by due change date.

For these reasons the ABA submits that an implementation period of at least 15 months and ideally up to 18 months for the general privacy reforms is made available to our members before commencement after all applicable regulatory measures described above have been finalised. This will ensure that both the Government and industry can be satisfied that the proposed reforms will be successfully implemented in an orderly manner minimising disruption to customers and business-as-usual processes.

The relatively recent example with the commencement of the personal property securities reforms under the Personal Property Securities Act 2009 (PPSA) provides the opportunity for an alternative commencement date model to be considered. With the PPSA the Government found it necessary to revert to the Parliament to amend the PPSA to give the Minister further scope to determine a later commencement date than the date fixed in the PPSA. This became necessary in order to avert a potentially premature and unsuccessful commencement of that regime. Fortunately, as things eventuated, this expanded power was not required to be used.

This model for determining a workable commencement date is attractive and would avoid a last minute deferral of commencement because of unforseen difficulties as was apprehended with the PPSA fixed commencement date.

The ABA submits that the Bill should be amended to provide for the responsible Minister to determine a commencement date of not less than between 15 and 18 months after Royal Assent once satisfied after consultation with industry that adequate time has been available to industry to implement and comply with the reforms.

4. Definitions/interpretation

4.1. Australian law

This is a new definition that is to be inserted into the Privacy Act (s6 (1)). In several of the APPs there are references to "Australian law" for the purposes of legitimising certain activities as "required or authorised by or under Australian law" (see for example APPs 2.2, 3.4(a), 3.7(a)(ii) 5.2(c). 8.1(c) etc)). Currently the NPPs provide that this exception applies where the activity is "required or authorised by or under law" (see for example NPPs 2.1(g), 6.1(h) and 10.2(b)(i)).

Banks are subject to compliance with a range of overseas laws that require personal information to be collected or disclosed in connection with Australian residents. An example is the US Foreign Accounts Tax Compliance Act 2010 (FATCA). According to a binding agreement with the US Internal Revenue Service Australian banks are required to identify and report on accounts held in Australia by US nationals and to collect information from Australian residents to determine whether they are US citizens.

Another example is the US Dodd-Frank Wall Street Reform and Consumer Protection Act that may require Australian financial institutions to report information about their customers to United States regulators.

It would be consistent with the ALRC's recommendation that the meaning of "Australian law" should be a clear, inclusive definition for the definition to include applicable foreign laws and arrangements such as under FATCA.

The ABA submits that the definition of Australian law should be extended to include any applicable overseas law or under a government agreement binding on an organisation.

4.2. Australian link

This definition is primarily concerned with the credit reporting provisions in Schedule 2 of the Bill and concerns specifically section 5B.

Given its importance this issue is raised by the ABA and ARCA.

Section 5B was inserted in the Act in 2000 when the Act was extended to apply to the private sector and to an act done or practice engaged in outside Australia relating to the personal information of an Australian citizen or a permanent resident.

The Bill makes a key change in section 5B so that the Act will apply extra-territorially without the need for the act or practice to relate to personal information of an Australian citizen or a permanent resident. This is a significant change to the extra-territorial operation of the Act. As the Explanatory Memorandum states, the Act will extend to every person, not just Australian citizens or permanent residents, so long as the entity dealing with the personal information has an Australian link.

Further, the Bill will impose an absolute prohibition on a credit provider's disclosure of credit eligibility information (as defined in Schedule 2) to an overseas recipient that does not have an Australian link, irrespective of the precautions that the disclosing entity has taken to ensure that the handling of that information is protected.

Conversely, APP 8 will regulate the cross border disclosure of personal information other than credit eligibility information to overseas recipients. While APP 8 will be more onerous for an entity than under existing NPP 9, the ABA supports in general the principle embodied in APP 8.

APP 8 together with proposed section 16C means a bank will remain liable if the overseas recipient of the personal information engages in conduct that would be a breach of an APP (other than APP 1) as if the conduct had occurred in Australia unless certain limited exceptions in APP 8.2 apply.

A bank's disclosure to an overseas recipient that is a related entity of the bank and which has an Australian link would be permitted but it appears not to an agent of the Australian entity if the agent does not have an Australian link.

The ABA is at a loss to explain why the disclosure of credit eligibility information to an overseas entity is to be so restricted and why the more practical APP 8 that deals with all other disclosures to overseas recipients is considered to be insufficient protection with respect to credit eligibility information.

The Explanatory Memorandum does not fully explain the policy reasons for this extension of the Act other than that is the objective to have an Australian credit reporting system.

An indication of the policy reasoning appears on page 91 of the Explanatory Memorandum that:

- the credit reporting system is to be restricted to information about consumer credit in Australia,
- the credit reporting system will not contain foreign credit information or information from foreign credit providers (even if they have provided credit to an individual who is in Australia), and
- information from the credit reporting system will not be available to foreign credit reporting bodies or foreign credit providers.

The ABA questions this reasoning.

Otherwise, there seems to be no logical reason why it is necessary for two different regimes to apply according to the type of personal information involved – the one, under the credit reporting provisions that imposes a complete prohibition on the disclosure of credit eligibility information to an overseas recipient where the recipient has no Australian link and the other, where the cross border disclosure of personal information other than credit eligibility information is subject to an accountability rule (section 16C) or specific exceptions.

These differences in a regulatory model that was intended to simplify the law and "to achieve greater logical consistency, simplicity and clarity" (see ALRC recommendation 5-2 that was accepted by the Government) will be operationally problematic for financial services businesses. This will mean that for purposes of disclosures to overseas recipients a bank will be required to separate credit information and personal information about a customer and manage the disclosures under different rules.

Further, the concept of an agency relationship between an entity with an Australian link and an overseas recipient acting as an agent for the Australian link entity does not appear to have been considered in this context. Agency has been considered within the Australian context in the Privacy Commissioner's Credit Reporting Fact Sheet 1: Credit Providers dated May 1996

(see http://www.privacy.gov.au/materials/types/factsheets/view/6488#3)

The Fact Sheet (in part) provides relevantly:

> *"Under the law, if a credit provider appoints an agent to carry out some of its functions in relation to assessing a loan application or managing a loan, the agent has the same access to credit information and responsibilities as the principal credit provider, but only in relation to the performance of those functions. This does not apply if the agent's function is to collect overdue payments on behalf of the credit provider. In other words, a debt collector is prohibited from gaining direct access to personal credit information kept by a credit reporting agency or another credit provider, when acting as an agent of a credit provider for the purpose of collecting overdue payments. Under the law, if a credit provider appoints an agent to carry out some of its functions in relation to assessing a loan application or managing a loan, the agent has the same access to credit information and responsibilities as the principal credit provider, but only in relation to the performance of those functions."*

The ABA submits that the disclosure of credit eligibility information to an overseas recipient should be regulated under APP 8 and not prohibited outright under a separate regime.

4.3. Pre –screening

Subsection 20(G)(1) has an express prohibition on the use by credit reporting agencies of credit reporting information for the purpose of direct marketing.

Subsection 20(G)(2)(c) has an exception in the case of a pre-screening activity provided consumer liability information and repayment history information (the new more comprehensive data sets) is not included in the activity.

The Explanatory Memorandum states that the purpose of pre-screening is to remove individuals from a direct marketing offer and not to allow credit providers to target identified individuals with direct marketing offers.

Pre-screening has not been defined in the Bill but is described in the Explanatory Memorandum (p138) as a "direct marketing process by which direct marketing credit offers to individuals are screened against limited categories of credit information about those individuals to remove (EM emphasis) individuals from the direct marketing credit offer..."

The ABA supports the direct marketing prohibition in subsection 20(G)(1).

It should be clear that the prohibition on the use of the new more comprehensive data sets should expressly cover both direct and indirect use in a pre-screening process.

Indirect use means using the new data sets as model inputs to derive an outcome. For example, a credit reporting agency may blend the data sets into a model to derive a credit propensity score that predicts a customer's likelihood to be receptive to an offer of credit. This predictor could then be used for pre-screening or direct marketing.

The ABA is supportive of the intent of these prohibitions which should be reflected clearly in revised Credit Reporting Code of Conduct and in the provisions of the Bill.

The ABA submits that it is made clear in the regulatory framework that the indirect use of consumer liability information and repayment history information cannot be used for direct marketing and pre-screening.

5. The APPs

The ABA's membership embraced the NPPs under the Act and found them to be workable for the mutual benefit of the bank and personal customers.

In this submission, our comments about the APPs are generally of a technical or workability nature. We believe that our comments do not challenge the fundamental policy objectives of the APPs. Similar to members' experiences in working with the NPPs, these comments are intended to ensure there are similar experiences and outcomes.

The ABA understands that the Government does not intend to propose regulations to deal with transitional aspects. It is noted that as a general comment, there does not appear to be any grandfathering or exclusions for existing personal information that was lawfully collected under the NPPs.

Areas where this may arise are the provisions in the APPs dealing with, for example, direct marketing (APP 7) and cross border disclosure of personal information (APP 8).

At this early stage of consideration of the Bill the ABA suggests that the Committee might provide its support for an investigation into the potential need for transitional regulations and to recommend that the Government takes this into account in the final settings of the legislation. Item 19 of Schedule 6 Part 7, makes provision for making transitional regulations. Currently, the Government does not propose to make transitional regulations.

5.1. APP 1 – open and transparent management of personal information

APP 1.4(g) will mean that a bank that is likely to disclose personal information to overseas recipients will have to list those countries in its privacy policy if it is practicable to do so. This requirement appears to be limited by the operation of section 13B where the disclosures are between related entities.

It may be practicable to list specific countries to where personal information could be disclosed by an Australian bank but it is unlikely that this would be reasonably practicable to do. The privacy policy will be required to disclose whether it is likely that personal information will be disclosed to overseas recipients. APP 8 will provide the protections for the individual if personal information is disclosed to an overseas recipient. The ABA questions the potentially prejudicial naming of recipient countries to which personal information may or may not be disclosed in light of the legislative protections that will be provided to individuals.

From an administrative perspective, it will be an onerous and costly obligation to keep a privacy policy up to date with this more specific information. By way of example, a bank will not control the location of an overseas server particularly if the server is moved or relocated without the bank's consent and where there may be multiple locations and where locations change quickly.

Also, for the operation of international payments systems where personal information, such as name, address, account number and possibly date of birth (when requested to satisfy sanction checks) is required to be provided to an overseas institution to complete a transaction, it should be clear in the Act that it would be impracticable to list every country to which a bank may need to remit payments. It is noted in the Explanatory Memorandum that APP 8.1 is not intended to apply where personal information is routed through servers that may be outside Australia, provided this information is not accessed by third parties. However, it should be clear that this would not be required for inclusion in a privacy policy as well.

Subject to the above, as a general comment, where listing of specific countries in disclosure documents is required under the APPs, the Act should make it clear that within these disclosure documents it is permitted to make reference that the policy is available on line (or by specified alternate means, for example, in a bank's branches). This would avoid potentially long lists of overseas jurisdictions being included in every document.

The ABA submits that APP 1.4 (g) should be amended to read "if it is reasonably practicable to specify". The word "reasonable" and "reasonably" are recognised expressions in the Act and the APPs.

5.2. APP 2 – anonymity and pseudonymity

The ABA supports APP 2 but notes that APP 2.1 states that individuals must have the option of not identifying themselves or using a pseudonym when dealing with an APP entity on a "particular matter". It will be important that organisations have access to guidance in the legislation or from the Privacy Commissioner about the meaning of "particular matter" given the mandatory nature of the individual having these options and for the purposes of financial services, where a provider is generally obliged by particular legislation to identify a customer.

5.3. APP 3 – collection of solicited personal information

The ability of an agency to collect (solicit) personal information from a third party does not apply to an APP entity such as a bank in order to authenticate an individual's identity such as under the Anti-money Laundering and Counter Terrorism Financing Act. The exception where the collection by the APP entity is required or authorised by or under an Australian law is not included in APP 3.

The ABA submits that the ability for an agency to collect personal information other than from the individual concerned should be extended to an organisation for the purposes of complying with a law relating to identification. The Explanatory Memorandum should provide these and other examples.

5.4. APP 4 – dealing with unsolicited personal information

There is a wide range of sources from which personal information filters into a large APP entity such as a bank.

It could be collected inadvertently through a bank's communications channels making it difficult and costly to quarantine this information that "could not have been collected" directly.

Possibly this obligation could be modified with an applicable "reasonable and practicable" test.

Under APP 4.3 APP entities are required to destroy or de-identify unsolicited personal information in certain circumstances but only if it is "lawful and reasonable" to do. The Explanatory Memorandum gives an example from the point of view of an enforcement agency. It would be useful to have an example clarifying that it would not be reasonable to destroy or de-identify unsolicited information which was, for example, part of a telephone call recording due to the difficulty in separating out the unsolicited information on the call from the solicited information on the call.

The ABA submits that some private sector examples should be included in the Explanatory Memorandum.

5.5. APP 5 – notification of the collection of personal information

Because the financial services sector is regulated under a wide variety of Australian laws (including certain overseas laws that have extra-territorial application) there is the risk that a requirement to provide an individual with a list of those laws will be onerous and very lengthy. APP 5 is tempered by the ability for an APP entity to take "such steps (if any) as are reasonable in the circumstances" and to notify the individual of matters "as are reasonable in the circumstances" or "to otherwise ensure the individual is aware of any such matters". It is unclear whether a lengthy list of laws would be unnecessary in certain circumstances and clarification would be welcome. An example of the significant volume of laws that affect financial institutions are statutory compulsions for production of documents. An important practical issue in the application of APP 5 is that it applies to the collection of personal information about an individual. This would cover situations where a bank suspects unlawful activity or misconduct is about to, or will, take place under, for example, the Anti-money Laundering and Counter - Terrorism Financing Act. Notification under APP 5 to the individual concerned would be inappropriate and could thwart potential action by law enforcement agencies but there is no provision for this in APP 5.

The only exception to notifying the individual of such matters in APP 5.2 is a general requirement to notify such matters as are reasonable in the circumstances or to ensure that the individual is aware of these matters. In practice, the exception for notifying the individual should be clearer by the addition of a "permitted general situation" type exception in APP 5.

Banks collect personal information from agencies on a regular basis about the hundreds of thousands of individuals on behalf of whom they execute international transfer payments. It would be costly and

impractical to notify each of those customers accordingly. Including a general statement in a bank's privacy policy should suffice.

1) The ABA submits that the Explanatory Memorandum should include a statement that a generic description such as "financial services laws" may be acceptable to obviate the need for a detailed list of all such laws.
2) In relation to the requirement in APP 5.2 (j) to notify the individual of the countries in which overseas recipients are located where the organisation is likely to be disclosing personal information, the ABA submits that the same approach as it has submitted in connection with APP 1.4 (g) should be followed.
3) APP 5 should make provision for circumstances where an organisation is not required to notify an individual of the collection of personal information about the individual including a "permitted general situation" exception and possibly an example in the Explanatory Memorandum dealing with the execution of international transfer payments.

5.6. APP 6 – use or disclosure of personal information

The ABA notes that where an APP entity collects personal information and passes it on to its related body corporate, that APP entity will be taken to have collected the personal information for the same primary purpose as the first mentioned APP entity. If the related body corporate seeks to use the information for a secondary purpose, the related entity must either obtain the individual's consent or fit within an exception in APP 6. Accordingly, a related body corporate is likely to need to consider wide encompassing privacy policies and notifications to ensure that all relevant primary purposes are covered to manage compliance with this and other APPs.

5.7. APP 7 – direct marketing

There is no definition of direct marketing in the Bill. The Explanatory Memorandum describes direct marketing as involving communicating directly with a consumer to promote the sale of goods and services to the consumer by a range of methods including mail, telephone, email or SMS.

The ABA doubts whether this statement adequately defines what "direct marketing" is.

The ABA submits that the term "direct marketing" should be given its ordinary meaning. The statement in the Explanatory Memorandum should be deleted or described as an example of what may be included in the meaning of "direct marketing".

The requirement to comply with a customer's request to disclose the source of information used or disclosed for direct marketing creates some practical issues despite the exception where the disclosure would be impracticable or unreasonable to do so.

In practice, it is likely that disclosing the source of the information will be impracticable or unreasonable in many cases if this APP were to be applied to personal information collected prior to commencement of the amendments where the organisation was not required to retain the source of the information.

Accordingly, what is considered to be "reasonable and practicable" would be critical for an organisation's compliance arrangements. Rather than leaving this question to the risk of differing interpretations, it should be made clear for the purposes of APP 7.6 and 7.7 that these provisions should apply only to personal information collected after commencement and not to pre-existing personal information held by the organisation. Please also note the ABA's submission later in this document under "6 – Transitional).

The ABA submits that APP 7.6 should be amended to provide that it (and APP 7.7.) applies only to personal information collected after commencement.

5.8. APP 8 – cross-border disclosure of personal information

APP 8 has to be read with proposed section 16C.

The ABA is concerned that the apparent intention with these provisions is that where -

- APP 8.1 applies to an APP entity that discloses personal information to an overseas recipient (i.e. that none of the factors in APP 8.2 apply to exclude the application of APP 8.1); and
- the overseas recipient is neither the APP entity nor the individual concerned; and
- the APPs do not apply to the conduct of the overseas recipient; and
- the overseas recipient engages in an act or practice that would breach the APPs (other than APP 1) as if the APPs had applied to the overseas recipient,

the APP entity will have no defence to a claim for liability for the breach by the overseas recipient of any of the APPs apart from APP 1 despite the APP entity having taken reasonable steps to ensure that the overseas recipient did not breach the APPs.

An APP entity that complies with the specific measures in APP 8.2 appears to be protected if the overseas recipient fails to comply with the APPs because APP 8.1 will not apply.

The ABA believes that a defence of taking reasonable steps should be available to the APP entity under APP 8.1.

The ABA submits that section 16C should be amended by adding after paragraph (b) of subsection 16C (1) "and (c) the APP entity has complied with Australian Privacy Principle 8.1; and".

For the purposes of APP 8.2(a)(i) and (ii) the Explanatory Memorandum provides that the reasonable belief test comprises information available to an APP entity and the context of the disclosure under APP 8.1.

In particular, if the defence above is not available to organisations, it will be essential that the exceptions in APP 8.2 (a) (i) and (ii) that provide for substantially similar laws or binding schemes that operate in those countries and that include the right of the individual to take action to enforce the protections of those laws or schemes law are free from doubt.

It would be helpful in the interests of certainty for both APP entities and individuals whose personal information is disclosed to overseas recipients for the Privacy Commissioner to publish and maintain a non-exhaustive list of countries that satisfy the reasonable belief test.

The ABA submits that the Bill should require the Commissioner to publish and maintain a non-exhaustive list of countries that satisfy the criteria in APP 8.2 (a)(i) and (ii).

The Explanatory Memorandum suggests that in applying the exception that the individual's consent has been given to the disclosure to the overseas recipient, it is not intended to apply in such a way that the individual's consent may be required before every proposed overseas disclosure is contemplated. This reading is readily open in APP 8.2(b) and is supported by the ABA as to do otherwise would be administratively onerous, costly and disruptive of normal processing of banking services. However the Explanatory Memorandum comments that "an individual has the explicit option of not consenting to certain disclosures that may include cross-border disclosures".

This is not an interpretation that is readily apparent from the terms of APP 8.2 (b).

The nature of some banking services are such that they may not be available to a customer without cross-border disclosures. If the customer has the option of withholding consent to these types of services the result may be that the service will be unavailable to that customer or continue to be made available to the customer unless other exceptions in APP 8.2 apply.

The ABA submits that the plain reading of APP 8.2(b) should not be conditioned by the quoted text in the Explanatory Memorandum.

Finally, it is unclear whether APP 8 will apply to pre-existing personal information that was collected prior to commencement that would necessitate retrospective disclosure to customers about their providing consent to these disclosures.

The ABA submits that existing NPP 6 should continue to regulate cross border data flows of personal information that had been held by the APP entity prior to commencement so that existing customer consents obtained prior to commencement are able to be relied upon.

Alternatively, existing consents should be grandfathered to allow orderly timing and opportunity for these to be updated in the ordinary course of business.

5.9. APP 9 – adoption, use or disclosure of government related identifiers

The ABA supports this APP 9 and has no further comment to make.

5.10. APP 10 – quality of personal information

The ABA supports this APP 10 and has no further comment to make.

5.11. APP 11 – security of personal information

The ABA supports this APP 11 and has no further comment to make.

5.12. APP 12 – access to personal information

APP 12 is substantially similar to NPP 6 except that "correction" is dealt with under APP 13.

However, APP 12.5 appears to require an APP entity despite having denied access to the individual to take such steps (if any) as are reasonable in the circumstances to provide access that meets the needs of the APP entity and the individual.

Banks can be expected to adopt an exhaustive process to accommodate the customer's access request. However, some guidance on the intended approach would be helpful.

The ABA submits that some examples about the approach to the provision of access in an alternative way that meets the needs of both parties could be included in the Explanatory Memorandum.

5.13. APP 13 – correction of personal information

In APP 13.5 and APP 12.4 there are requirements for an APP entity to respond to an individual's request for access or correction of his or her personal information within a reasonable time.

The ABA supports this approach. One point to mention is that banks and other financial services providers are subject to a number of regulatory requirements under the law, under regulatory instruments issued by the Australian Securities and Investments Commission (ASIC), under ASIC's Electronic Funds Transfer Code of Conduct (re-named "e-Payments Code) and the Code of Banking Practice to comply with certain specific timeframes and complaints procedures when dealing with customers.

Banks have implemented internal processes and systems to ensure that they comply with these regulatory timeframes and processes.

The ABA is concerned to ensure that compliance with these timeframes is taken into account when determining what is or is not a "reasonable time" in any given circumstance.

The Privacy Commissioner may assist in this by developing guidance in consultation with the financial services industry for recognition of these compliance measures.

6. Transitional

According to section 2 of the Bill, Schedule 1 commences on the day after the end of the 9 months period commencing on Royal Assent. There is a notable absence of broad ranging transitional provisions in the Bill, although provision is made in the Bill for transitional issues to be dealt with by regulations. At this stage the Government is not proposing any transitional provisions in addition to those in Schedule 6 Part 7 of the Bill.

Clearly, this is an important aspect of any amending law and should be free from doubt for organisations that must comply with new or amended rules.

One simple approach to determining whether some of the amendments in the Bill will apply to pre-existing personal information that is held by a bank and to personal information that is collected after commencement of the legislation, is to take the words "holds" and "collects" in the APPs respectively and deciding that "holds" indicates all pre and post personal information is affected, and that "collects indicates only prospective activity.

As a rule of thumb this is useful but as a rule of compliance it is inadequate.

For example, on the simple approach, APP 4 creates no obligation to distinguish solicited from unsolicited personal information that was received prior to commencement. This is a sensible and practical approach because for an APP entity to go back to the point when personal information had been received and to differentiate whether the information had been solicited would be a major and costly exercise.

Other APPs seem to apply to existing personal information that had been collected or prior to commencement, such as in APPs 6, 7, 8, and 11. APP 9 (adoption of government identifiers) seems to apply to existing and future acquired information.

For example, in APP 7.6 an individual is able to request an APP entity to provide the source of the individual's personal information which had been used or disclosed for direct marketing. APP 7.6 makes no distinction between pre-existing personal information that is subsequently used or disclosed and personal information that had been collected after commencement. In APP 7.6 this is a critical distinction because banks normally would not have recorded the sources of each piece of personal information they had collected in the past and continue to hold and could not be expected to ever comply with this requirement for existing customers. In the result, reliance on the exception in APP 7.7(b) would become the norm with all requests from existing customers likely to be refused.

The ABA submits that the issue of which aspects of the APPs apply before and on commencement should be put beyond doubt and that transitional provisions should be made accordingly.

Another key transitional concern arises under the informed consent exception in APP 8.2 (b). This is mentioned above under our comments on APP 8 generally. On the above analysis it seems that the consent exception in APP 8.2(b) will apply in all cases of both existing and new customers' personal information that may be sent to an overseas recipient. Therefore, APP 8.2(b) will mean a change to banks' privacy consent forms where a bank wishes to rely on a customer's consent for the bank to send personal information to an overseas recipient. This change will entail the bank expressly informing the customer that if the customer consents to the disclosure to an overseas recipient APP 8.1 will not apply.

Presumably, the bank would have to explain the effect of APP 8.1 not applying to the customer. This is a very significant change to the current consent exception under NPP 9.

In order for APP entities to manage this cost effectively and conveniently for their existing customers the ABA recommends that NPP 9 should continue to apply to the financial products and services that have been provided to the customer prior to commencement or alternatively, and more easily determined, to existing customers immediately prior to the time of commencement.

For new customers or new products and services to be provided to existing customers after commencement APP 8.2(b) would apply.

Alternatively, where an updated privacy consent is required for compliance with APP 8.2 (b) a transitional arrangement should be provided so that for existing customers the updated consent form can be provided over a reasonable period of time in the ordinary course of business of a bank's communications with its customers after commencement.

7. Complaints

Part V "Investigations etc" in the Privacy Act is to be amended to include a number of new provisions.

The ABA is concerned that Item 93 in Schedule 4 of the Bill dispenses with the requirement for the Commissioner to conduct an investigation in private, but to do so only in the Commissioner's discretion. The ABA agrees with the statement in the Explanatory Memorandum that this change would enhance the Government's ongoing transparency and open government reforms but disagrees that this should apply equally to private sector organisations.

Complaints handling can involve commercial-in-confidence information, expose individuals, including employees, to the risk of personal criticism and harm commercial reputations if this information is aired in public, irrespective of the outcome.

Further, this change appears to be inconsistent with proposed section 16A under which an APP entity may collect, use and disclose personal information for the purposes of a confidential alternative dispute resolution process.

The Commissioner will have the power to recognise external dispute resolution schemes (REDRs) and may decide not to investigate a complaint if he or she is satisfied the complaint is being dealt with by a REDR. It is expected that the power to recognise a REDR would require the Commissioner to be satisfied that the REDR is able to conduct its processes confidentially otherwise a respondent organisation may be unable to disclose personal information about the complainant in its defence.

The ABA submits that privacy complaints against private sector organisations should be dealt with in private. Item 93 should be amended to provide that the Commissioner's discretion whether to conduct an investigation in private applies only to a complaint about an agency. Otherwise, the investigation must be held in private.

8. Penalties

Section 13G provides for a civil penalty for "a serious interference with the privacy of an individual" or "repeatedly does an act, or engages in a practice that is an interference with the privacy of one or more individuals". The penalty is 2,000 penalty units.

Below under "9 - Enforcement" the ABA submits that there should be a general defence available to an APP entity.

Further, consideration should be given to the Bill establishing a more proportionate civil penalty response to an infringement of privacy that is substantially less than is currently proposed.

9. Enforcement

Enforcement of the Commissioner's determination that an APP entity has breached the Act must be by *de novo* hearing by the court.

The Act does not have legislated defences to either the claim that an APP entity has committed an interference with the privacy of the individual or that can be raised in a subsequent court proceeding.

The amendments in the Bill will create a more onerous compliance regime for APP entities in the collection, handling, use and disclosure of personal information.

Banking is a highly dynamic environment for the handling of personal information across a very large number of employees. Banks will continue to develop and implement robust privacy protection systems and processes and will rigorously train staff as they have done to date.

Inadvertent breaches of the Act and the APPs may occur in circumstances where these occurrences ought fairly to be excused.

The ABA submits that the Act should include a defence of inadvertence where the Commissioner and the court may conclude that the person concerned acted honestly and reasonably and in the circumstances ought fairly to be excused.

10. Concluding comments

The Bill contemplates significant changes to Australia's privacy laws, particularly the credit reporting regime.

The ABA supports a sound privacy protection regime for Australian individuals and reiterates its support in welcoming the Government's lead for the introduction of a more comprehensive credit reporting system in Australia.

A key factor for the Government, industry and consumers to realise a successful implementation of the regime is to ensure the private sector has adequate time to prepare for and comply with the regime with the Government establishing a realistic commencement date mechanism

In addition, the ABA would like to see the Government undertaking an effective public information campaign in consultation with the credit and broader financial services industry before the changes take effect, with the object of shaping the community's expectations of the benefits and protections that will be afforded to individuals, particularly with respect to the enhanced credit reporting regime.

Yours sincerely,

Steven Münchenberg