**A**USTRALIAN **B**ANKERS' **A**SSOCIATION INC.

Steven Münchenberg
Chief Executive Officer

Level 3, 56 Pitt Street
Sydney NSW 2000
Telephone: (02) 8298 0401
Facsimile: (02) 8298 0447

9 August 2010

Ms Christine McDonald
Committee Secretary
Senate Finance and Public
Administration Committee
PO Box 6100
Parliament House
CANBERRA ACT 2600

Email to: fpa.sen@aph.gov.au

Dear Ms McDonald,

## Exposure Draft of Australian Privacy Principles and Companion Guide

The Australian Bankers' Association (ABA) is pleased to see the release of the Australian Privacy Principles (APPs) in Exposure Draft and for the opportunity to contribute to their consideration by this Senate Committee. The ABA is appreciative of the additional time granted to provide this submission.

The ABA is the peak national body representing 23 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 bank subsidiaries and retail, formerly regional, but now nationally operating banks.

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 APPs are a welcome development towards a more seamless and nationally focused Australian privacy regime that the ABA and its members have looked forward to for some time.

The ABA's involvement with the national privacy regime goes 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 that were enacted in 2000.

## Introduction

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

The duty of confidentiality which is a duty not to disclose a bank customer's affairs unless certain exceptions apply 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 its customer relationship. 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.

A bank will have subsidiaries that provide additional financial services to complement the bank and customer relationship such as general insurance, financial advisory and investment services where some personal information sharing between these entities is necessary.

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 the 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 and compliance with privacy and other laws that apply to financial services activities.

The APPs have broken down some of the NPPs into discrete elements where the need to do so has been seen. This segmentation will mean additional compliance programs for banks adding costs to a bank's management of customer information and the customer relationship. For example, a separate direct market principle (APP 7) has been developed to replace the existing direct marketing provisions in NPP 2.1 (c) of the Privacy Act. APP 7 is intended to distinguish between existing customer relationships and those where direct marketing is made to other consumers. The ABA supports this distinction but later in this submission we will explain why the current drafting may not achieve this objective.

---

[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

## ABA's Comments on the APPs

### 1. APP 1- open and transparent management of personal information

APP 1 is an expanded version of existing NPP5 (the Openness Principle).

APP 1 prescribes seven elements as the minimum content of an organisation's privacy policy. The prescribed information includes whether the organisation is likely to disclose personal information to an overseas recipient who is not in Australia and is neither the individual concerned nor the organisation itself and to specify the relevant countries if practicable.

The ABA disagrees with the requirement to list relevant countries in an organisation's privacy policy.

To comply with this obligation, this information can only be provided confidently where a bank has created established overseas recipients, including a related entity of the bank, that perform services, processing or activities for the bank.

Where the bank does not control the location of an overseas server the bank is exposed to the risk of non-compliance if the server is relocated without the bank's knowledge. This could occur frequently.

The requirement to list relevant countries would be an onerous and costly obligation because of the need to continually monitor developments and amend the list as circumstances change. The ABA questions the value of this information that is to be provided to an individual given that APP 8 deals specifically with cross-border disclosures of personal information.

This disclosure contains an underlying inference or an invitation for the individual to draw the inference that a named overseas country of the intended overseas recipient is not to be trusted with the personal information. This would be an unfortunate signal for Australia's law to send internationally.

If the requirement to list relevant countries is retained, it should be made clear that this requirement in APP 1 applies where the bank chooses to send personal information overseas for processing or receipt of another service. APP 1 should not apply where an individual initiates a transaction that the individual indicates is destined for a recipient in an overseas country, for example a payment to a relative overseas that is processed by an Australian bank to its correspondent bank in the country of destination.

Subject to the above comments, the ABA suggests that in sub-section 2 (4)(g) the words "reasonable and" are added before the word "practicable". This is to take account of potential volatility in the location of servers in other countries that could be numerous and where locations change quickly.

## 2. APP 2- anonymity and pseudonymity

The ABA supports the clearer explanation in this principle of the circumstances where an organisation may decline a customer's request to transaction anonymously or by using a pseudonym.

Clearly, for many reasons, including a bank's obligations under anti-money laundering, counter terrorism and financial transaction reporting laws, these options for customers are not available.

## 3. APP 3 – collection of solicited personal information

The ABA supports the general principle that information should be solicited only for purposes reasonably necessary for or directly related to an organisation's functions or activities.

The ABA agrees that ideally personal information ought to be collected only from the relevant individual unless it is unreasonable or impracticable to do so.

The ABA suggests that sub-section 4(5) is amended to add a further exception to allow organisations to obtain information from third parties in order to authenticate a customer's identity. This recognises the increased use of third party verification methods to satisfy legislative requirements, such as anti-money laundering and counter terrorism legislation.

Further, there will be cases where an individual who is not able to understand English is assisted by a third party where a bank's multilingual staff are temporarily unavailable.

In respect of the collection of sensitive information from a third party where the individual concerned has consented to the collection it should be clear that this is not prohibited under this sub-section 4(5).

## 4. APP 4 – receiving unsolicited personal information

The passive receipt of personal information is part of NPP 1 because it applied to collection from any source.

The ABA is concerned with the segmentation of the receipt of personal information by an organisation into circumstances where the information is solicited and where it is not. The segmentation will create additional compliance obligations and compliance costs without clear benefit to privacy principles.

The ABA submits the treatment of the collection of personal information, whether directly or indirectly, should be dealt with under a single principle which merges APP 3 with APP 4 subject to certain amendments below.

APP 4 imposes a potentially significant additional compliance burden on an organisation. The organisation must within a reasonable period determine whether the organisation could have obtained the personal information from the individual for the purpose of complying with APPs 5 to 13.

The organisation must also determine whether it could not have collected the personal information at all and if so the organisation must destroy or de-identify the information if it would be lawful or reasonable to do so.

The wide range of potential sources of information coming into an organisation the size of a bank and its customer base, and the training of thousands of staff to recognise that the receipt of certain information may require the determination to be made as required under APP 4, will be a very significant practical exercise.

What is determined to be "within a reasonable period" must take account of the dimensions of this obligation to make the requisite determination. The ABA suggests that APP 4 is clarified by a legislative note or that the period is clarified by guidance from the Privacy Commissioner to assist in resolving any uncertainty.

A further clarification is required to APP 4 sub-section 5(4) so that the words "could not have collected" means that the collection is prohibited by law rather than simply because it is information that the individual could not provide, for example, the opinion given by a third party or information that is obtained in connection with an insurance claim where the insured's duty of disclosure is in issue.

The ABA submits that a proportionate and workable approach to the application of this principle would be to require that the obligation to destroy or de-identify personal information applies only to unsolicited information received from third parties rather than from the individual concerned.

The ABA believes the unbundling of NPP 1 into two discrete principles should be reconsidered.

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

APP 5 sub-section 6 (1) expands slightly the notification aspects under NPP 1.3 and NPP 1.5 for the organisation to take such steps (if any) that are reasonable in the circumstances to positively notify the individual of the collection and the prescribed matters under APP 5 sub-section 6 (2) or otherwise to ensure the individual is aware of these matters.

APP 5 sub-section 6 (2) adds to the list of prescribed matters under NPP 1.5.

APP 5 sub-section 6 (1)(b) requires the organisation to ensure that the individual is aware of the collection from another person and the circumstances of the collection as specified in APP 5 sub-section 6 (2)(b). While this obligation is to the extent that is reasonable in the circumstances, the ABA is concerned that this requirement is an absolute obligation. It could involve the disclosure of information by which the identity of the third person could be determined, which could be an issue of confidentiality or privacy for the third person. For example, the third person could provide an opinion to an organisation as to the suitability of the relevant individual for employment with the organisation, but the individual is declined employment and therefore the record does not become part of the employee records exemption.

The ABA suggests that similarly to APP sub-section 12 (3)(b), the obligation in APP 5 sub-section 6 (2)(b) should provide that disclosure should not have an unreasonable impact on the privacy of other individuals.

The obligation to notify the individual of any applicable law that authorises or requires collection of the information is onerous and of little assistance to the individual unless the individual knows the particular provisions of each law.

Given the wide range of financial services laws applying to banks and other financial services providers, it should be sufficient for a bank to state generally that certain of the information that is solicited from the individual will be for the purposes of the bank's compliance with financial services laws. For example, after 31 December 2010 under the *National Consumer Credit Protection Act 2009* (NCCPA), a bank when considering its customer's loan application must

- make reasonable inquiries about the customer's requirements and objectives;
- make reasonable inquiries about the customer's financial situation;
- take reasonable steps to verify the customer's financial situation.

In passing it is noted that some of the information that is to be verified may have to be vouched not by the individual but from other sources, for example the individual's employer.

If the customer requires only a credit facility then a bank would have to specify the NCCPA in its notification, together with any applicable law of a general nature such as the *Anti-money Laundering and Counter-Terrorism Financing Act 2006, the Privacy Act* and so on. Different disclosures of applicable laws would then need to be provided for non-consumer credit products, as the NCCPA would not apply to those products. Similarly, other disclosures might be required for deposit products. Unless the bank is able to provide a generic statement about information that is collected pursuant to a non-specific range of financial services laws this would mean that it could not develop a standard form notification document. This would add significantly to costs and of questionable benefit to the individual.

It would be misleading to include specific laws that do not apply.

Further, a complete list of applicable laws would be very long. In addition to financial services laws there are, for example, a number of relevant revenue collections laws applicable in all nine Australian jurisdictions depending upon the jurisdiction in which a particular transaction occurs and where information is required to be provided to the revenue authority.

For these reasons the ABA considers that a generic statement about laws that authorise or require collection of personal information in the case of financial services should be able to be notified as primarily the basis for collection without identifying each of those individual laws.

The ABA refers to and repeats its concerns over the requirement that an organisation should notify the individual whether it is likely that the personal information will be disclosed to an overseas recipient and to name the country or countries concerned if practicable.

This requirement appears in APP 1 with respect to a privacy policy and in this APP 5. There is uncertainty whether this disclosure has the same meaning in APP 5 as it may mean in APP 1. It could be open to argue that because APP 5 applies to information that is about to be or has been collected the disclosure requirement is intended to be more specific than under APP 1 where the nature of the information is unknown. This would be a major compliance burden for an organisation to make a more specific notification about the likelihood of personal information being disclosed to an overseas recipient.

APP 8 provides a comprehensive and timely model for the accountability of entities for cross-border disclosures. It focuses on the potential risk to the individual of the cross-border disclosure and the protections that apply for the customer. This would be more relevant and important to the individual than the generally vague statements in both the privacy policy and under the notification principle APP 5 (with their potentially undesirable inferences) that information might be disclosed to an overseas recipient.

## 6. APP 6 – use or disclosure of personal information

APP 6 sub-section 7 (1) differs from NPP 2 in referring to the primary purpose of collection as a "particular purpose".

This raises a concern for financial services providers.

Generally speaking, when an individual acquires a financial service as a customer of the bank there is an ongoing relationship that in many cases lasts until one of them ends the relationship.

In the course of that relationship there will be a range of different activities including providing the customer with statements of account, notifying the customer of changes such as to terms and conditions, applicable fees and interest, ongoing information that is required or desirable to be provided relating to some of the security aspects of the facility, dealing with complaints and the potential for a complaint to proceed to an external dispute resolution scheme and, in the case of a default under a credit facility, the need for collection activity.

The reference to "a particular purpose" should be clear it encompasses all necessary or naturally related purposes. For example, the particular purpose of processing a loan application should include all of the possible activities and use and disclosures of personal information that are necessary to maintain, service and recover the loan. It should be clarified that all necessary or naturally related purposes are able to be described in this way and are taken to be included in the meaning of "particular purpose". The lengthy list of exceptions in APP 6 sub-section 7 (2) are welcome and practical.

However, compared with the reference to "particular purpose" in APP 6 sub-section 7(1), sub-sections 7(2)(h) and (i) suggest that the wider approach to activities associated with "particular purpose" in the case of financial services might not be available .

The ABA believes that this uncertainty should be examined and addressed as we have indicated.

A disclosure under sub-section (2)(d)(i) is limited to the relationship that the actual or intended conduct has with the organisation's functions or activities.

The ABA believes that this limited application of this exception requires closer examination. In the context of the public interest and "whistleblower" protections, entities should have some discretion to disclose information about potential unlawful activity or serious misconduct even if it doesn't relate directly to their own functions and activities.

## 7. APP 7 – direct marketing

The ABA supports the separate direct marketing principle because it will be able to provide a clearer model for direct marketing in a privacy context.

As a preliminary observation, the ABA notes that "direct marketing" has not been defined. This is currently the case under NPP 2.1 (c).

However, the references in sub-section 8(6) to the *Do Not Call Register Act 2006, the Spam Act 2003* and any other prescribed Commonwealth Act suggest that "direct marketing" in APP 7 is confined to direct marketing by means other than the means covered under those Acts.

To avoid possible confusion between APP 7 and the operation of those Acts referred to in sub-section 8(6), the ABA recommends that consideration is given to aligning APP 7 with the pivotal concept of "inferred consent" in the *Do Not Call Register Act 2006 and Spam Act 2003.*

The Companion Guide to the Australian Privacy Principles (Companion Guide) describes the intended policy approach to APP 7 as being to distinguish direct marketing to existing customers from direct marketing to non-existing customers.

From a compliance aspect this is a helpful distinction. The distinction between existing and non-existing customers becomes confused by the provisions of APP 7 (3)(a)(i) that suggest that the personal information, although collected from an existing customer by the organisation, must be handled differently because that individual would not reasonably expect the information to be used by the organisation for direct marketing. The advantage of the distinction between existing and non-existing customers is therefore significantly lost.

By comparison the *Do Not Call Register Act 2006* provides a clearer exception for an organisation whose customer registers his or her telephone number on the Register to contact the customer by telephone for marketing purposes.

This exception is based on the inference of consent from the existing business relationship between the customer and the organisation. It is another reason why the "inferred consent" model is more suited to the direct marketing principle APP 8.

From an industry compliance aspect, there should be recognition of the inter-relationship between many of the APPs and the increased emphasis in APP 1 on the more detailed disclosure requirements of an organisation's privacy policy.

This approach would mean that the obligation on the organisation under APP 1 sub-section 2 (4)(c) to disclose the purposes for which the organisation "collects, holds, uses and discloses personal information" would be taken into account in determining whether an individual "would not reasonably expect the organisation to use or disclose the information" for the purpose of direct marketing (APP 7 sub-section 8 (3)(a)(i)). Otherwise, what value is there in the requirement for the particular disclosure in the privacy policy?

An issue arises under the proposed wording of APP 7 sub-section 8 (2)(a) for some members, specifically in relation to aggregation products. These products typically involve an agreement with the customer to source and aggregate financial information about the customer from the customer's other financial institutions using the customer's credentials. Information acquired this way is compiled into financial statements and can be made available to the customer in a useful format in secure internet banking sessions.

The customer provides his or her credentials for this express purpose, and informed consent to the collection and aggregation of the customer's information from third parties underpins the arrangement.

As part of the terms of these products, the bank may make use of this information for marketing purposes. In many cases the marketing may be presented in tailored product offers appearing during internet banking sessions, rather than through traditional 'communications'.

The proposed wording of APP 7 would require excessive disclosure of the customer's right to opt out in these circumstances. The ABA suggests changing APP 7 to read as follows (amendment in red):

*"Personal information collected from, or with the consent of, the individual*

(2) This subsection applies in relation to the use or disclosure by an organisation of personal information about an individual for the purpose of direct marketing if:

(a) The organisation collected the information from, or with the consent of, the individual; and

(b) The individual would reasonably expect the organisation to use or disclose the information for that purpose; and

(c) The organisation provides a simple means by which the individual may easily request not to received direct marketing communications from the organisation; and

(d) The individual has not made such a request to the organisation.

*Personal information collected from another person etc*

(3) This subsection applies in relation to the use or disclosure by an organisation of personal information about an individual for the purpose of direct marketing if:

a) the organisation collected the information:

i. from, or with the consent of, the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or

ii. from a person other than the individual or without the consent of the individual; and

b)

i. the individual has consented to the use or disclosure of the information for that purpose; or

ii. it is impracticable to obtain that consent; or

iii. the individual has been notified of the use or disclosure of the information for that purpose and the individual hasn't objected to that use or disclosure; and

c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

d)

i. in each direct marketing communication with the individual, the organisation includes a prominent statement that the individual may make such a request; or

ii. the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and

f) the individual has not made such a request to the organisation."

In APP 7 sub-section 8 (4) an organisation may consider it preferable in managing its customer relationship for it to provide a composite option for its customer to request not to receive direct marketing at all from any source instead of selective options in the way they are listed in APP 7 sub-section 8 (4)(a),(b) and (c).

The ABA requests that this is clarified so that this approach is available.

Finally, the ABA submits that the requirement for the organisation to provide its source of information should be limited to requests by non-existing customers.

Existing customers will already be aware (e.g. from the privacy policy) that the bank obtains information from various sources and will already have had the chance to opt-out of direct marketing if they want to. Requiring banks to keep track of and retrieve source information for existing customers who welcome direct marketing seems an unwarranted compliance burden.

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

This principle makes some significant changes to the approach taken with NPP 9. Primarily the NPP 9 approach is a prohibition on cross-border transfers of personal information subject to certain prescribed exceptions.

The approach under APP 8 replaces this prohibition with an accountability model that will not prohibit disclosures of personal information to overseas recipients. It simply ensures that the disclosing organisation is accountable for the protection of the information subject to certain limited exceptions.

The ABA supports this model on the basis that it is commercially and socially realistic.

There are some aspects of the principle that the ABA believes require further consideration including some aspects of the drafting and approach.

The reference in APP 8 (1) to "breach" is questionable because presumably the overseas recipient is not bound in a legal sense by the APPs under Australian law unless the overseas organisation has an Australian link as defined in the Exposure Draft.

**Appropriate limitations to strict liability**

Under sub-section 20 (1)(d) if the APPs do not apply to an overseas recipient as provided under APP 9 sub-section 9 (1), then any act done or practice engaged by that overseas recipient that would be a breach of the APPs (other than APP 1) if the APPs applied to that act or practice will be taken to have been done or engaged in by the organisation that will then be accountable for that "breach".

Accountability for a third party's breach arises irrespective of what steps the Australian data custodian might have taken to secure compliance with the APPs under APP 8 (1).

The ABA considers it unreasonable for its members to face the risk of prosecution and liability for penalties where they have taken reasonable steps to ensure that the overseas recipient did not "breach" the APPs (other than APP 1). The ABA suggests that section 20 (2) is qualified by limiting the words 'for the purposes of this Act' to refer to the purposes of the compensation, rather than penalty, provisions of the Act.

The ABA is also concerned that as worded, Section 20 may permit an overseas data custodian who has breached the APPs through failure to take care on its part to limit its liability to the Australian data collector under Australia's proportionate liability laws.

These laws were introduced by State and Federal Governments to limit liability in negligence based cases (whether in tort or contract) to each party's respective degree of fault. The purpose of these reforms was to ensure that indemnity insurance remains affordable.

Unless section 20 is qualified, it may be possible for an overseas recipient that has failed to take adequate care of personal information to seek to limit its liability to indemnify an Australian data sender in respect of liability to Australian data subjects by invoking proportionate liability.

The ABA supports the compliance test in sub-section 9 (1) that is informed by the Companion Guide. It is customary for banks that transfer personal information to an overseas recipient to have contractual arrangements with the overseas recipient that oblige the recipient to observe Australian law. The Companion Guide supports the existence of these arrangements as appropriate in assessing whether an organisation has taken "such steps as are reasonable in the circumstances" as required by the sub-section.

Where these steps are taken, no penalties should be imposed and no barriers created to the organisation enforcing contractually allocated responsibilities for secure data management.

**Transfers that are obvious and necessary**

There is a wide range of commonplace international transactions in which it is obvious that information will cross international borders but where it is not practicable for the ABA's members to impose any controls on the recipients. These include international payments and international credit card transactions.

The ABA is concerned its members may face difficulty in meeting the exception in sub-section 9 (2)(b) in all such instances and seeks an additional exception to section 9(1) where an overseas transfer of information is a necessary step in providing a service which would be obvious to a reasonable person turning their mind to the circumstances.

An everyday example is the case of an Australian bank customer who wishes to use his or her credit card overseas. To do so, their Australian credit card issuer (bank) must confirm the availability of credit to the overseas merchant. This is an obvious and necessary disclosure of personal information. The exception in sub-section 9 (2)(b) applies where consent of the individual is obtained, but only if the individual is expressly informed that if the individual consents the cross border principle in APP 8 will not apply. This exception will be dependent on how the Privacy Commissioner interprets "expressly informs". If a bank must separately and individually expressly inform each customer whose personal information is to be disclosed to an overseas recipient the consent exception will, in all practicality, be illusory.

The reality for a bank or other organisations that have a large number of customers, in the case of a bank in the millions, the batch processing of transaction data would become practically impossible because an individual's data cannot be conveniently removed from the batch.

The bank customer who wishes to use his or her credit card overseas faces a difficulty if the bank cannot assume from the date of the issuance of the credit card facility that the customer has consented to the bank disclosing transaction information to the acquiring financial institution of the overseas merchant.

Otherwise, the customer would have to seek permission of the bank to use the credit card overseas which would be inconsistent with the flexible and convenient nature of a credit card facility and the customer's expectations.

Further, the reference to "affected individual" in sub-section 9 (2) and in 9 (2)(b) suggests that the individual is not merely an individual who potentially may be affected. Arguably, it contemplates knowledge at the time that the particular individual is to be affected; that is, the individual's personal information is to be disclosed to an overseas recipient.

If this is the correct interpretation, then this adds to the illusory nature of the informed consent exception, because the obligation to expressly inform the individual and to obtain the individual's consent would be required in every case of personal information that is known to be provided to an overseas recipient.

Sub-section 3 (b)(iii) of the Privacy Amendment (Private Sector) Act 2000 provides that one of the main objects of the Act is to regulate private sector organisations in a way that:

> *(iii) recognises important human rights and social interests that compete with privacy, including the general desirability of a free flow of information (through the media and otherwise) and the right of business to achieve its objectives efficiently".*

It would be consistent with this policy objective for it to be clear that an organisation "expressly informs" its customer by providing the prescribed information in its privacy policy so that the customer knows that in choosing to deal, or to continue to deal, with the organisation the individual consents to the potentiality of his or her personal information being sent to an overseas recipient.

One of the exceptions to APP 8 sub-section 9 (1) is where the organisation reasonably believes that the overseas recipient is subject to substantially similar regulatory requirements as the APPs and there are mechanisms that allow the individual whose information is being sent overseas to enforce that protection.

As these are objective tests, it would make sense for this to be determined by the Privacy Commissioner so that entities are not left uncertain about whether this test is met or not and unnecessary assessments and inconsistent conclusions within industry are avoided. The ABA recommends that the Privacy Commissioner (to become the Australian Information Commissioner) provides guidance or rulings on overseas countries that have a law or binding scheme that satisfy the requirements of sub-sections 9 (2)(a)(i) and (ii).

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

The ABA notes that APP 9 appears to be based on NPP 7 with some modifications that provide greater flexibility for use and disclosure in certain situations.

In sub-section 10 (3) there is the reference to compliance with regulations that may be prescribed for the purposes of APP 9.

There is no indication of whether any regulations are intended to be made.

It would be helpful closer to the finalisation of the legislation if this could be indicated to assist with our members' implementation programs.

The ABA has no further comments to make on this principle at this stage.

## 10. APP 10 – quality of personal information

The ABA notes that this principle reflects the obligations under NPP 4 relating to the collection, use and disclosure of personal information and makes no further comments on this principle at this stage.

## 11. APP 11 – security of personal information

The ABA notes the omission in this principle of the references in some other APPs to the taking "such steps (if any) as are reasonable...".

By contrast, APP 11 requires that an organisation "must take such steps as are reasonable in the circumstances".

Banks are very concerned to ensure that their systems, retained information and processes are secure and that their customers have confidence in the integrity of these arrangements.

The ABA welcomes the stronger emphasis in APP 11 on organisations to take all reasonable steps to ensure their systems and processes are secure.

A new element, "interference" has been added to this principle that is not present in NPP 4.

It is unclear what this additional factor is intended to address. It did not appear in the factors recommended by the Australian Law Reform Commission in its Report 108 dated May 2008 "For Your Information" (Report 108) and was not mentioned in the Government's First Stage Response to Report 108.

The Privacy Commissioner should consider providing specific guidance, with examples, of how "interference" might occur and differ from the other stated factors in APP 11 of "misuse", "unauthorised access" and "modification".

## 12. APP 12 – access to personal information

The general approach to access in this principle reflects the approach under NPP 6 that access should be provided on request (within a reasonable period of the making of the request).

The exceptions for providing access generally follow those in NPP 6.

A new factor in APP 12 that is not included in NPP 6 is the case where the organisation declines to provide access in the manner requested by the individual.

The ABA believes that the requirement to give reasons for the refusal on this ground, together with the provisions of sub-section 13 (5) (other means of access) should provide, in the majority of cases, a workable outcome and avoid escalation of any disagreement.

The ABA has no further comments to make on this principle at this stage.

## 13. APP 13 – correction of personal information

There is a possible change and significant shift in emphasis in this principle compared with NPP 6.

In NPP 6, in order to trigger an obligation on the part of the organisation to correct information, the individual is required to establish that the personal information held by the organisation is not accurate, complete and up-to-date.

In APP 13, sub-section 14 (1)(b)(i) states if

> *(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete or irrelevant;"*

the obligation on the organisation is to take such reasonable steps (if any) as are reasonable in the circumstances to correct the information.

Depending on how this obligation is interpreted, one interpretation could lead to an organisation being under an obligation to continuously monitor and review personal information that it holds whether prompted to do so or not. The ABA believes that this is not the intention of this principle and should be clarified in APP 13.

In light of documentary retention laws and statutes of limitation, a bank must be able to comply with this obligation through appropriate review processes, reasonably designed to address the risk of obsolete information being used in a way that may disadvantage or harm the subject.

Otherwise, the costs to banks of routinely reviewing personal information held by them compared to the negligible benefit to their customers would be unjustifiable on any costs and benefits assessment.

In support of this view, APP 10 (information quality) prompts an organisation to ensure that personal information when it is used or disclosed is accurate, up-to-date, complete and relevant.

The Companion Guide also seems to support this approach in its reference to the ability of an individual to be put in control of personal information through an online facility.

Otherwise, the ABA submits that sub-section 14 (1)(b)(i) is amended by adding after "satisfied" the words "by the individual or another person authorised by the individual" to address this matter.

## Definitions

In accordance with the ABA's recommendation with respect to APP 7 (direct marketing), the definition of "consent" for the purposes of APP 7 only should be defined as "inferred consent" based on the definitions in the *Do Not Call Register Act 2006 and Spam Act 2003.*

## Concluding comment

The recent series of reviews of privacy law in Australia has entailed an exhaustive examination of law and practice that the ABA looks forward to setting a longer term, stable benchmark for privacy protection that accommodates legitimate business needs and practices in an increasing borderless environment.

The work of the Asia-Pacific Economic Cooperation Privacy Framework will be an increasingly important contribution to Australia's privacy policy.

The ABA also looks forward to ongoing consideration of how sectoral aspects of privacy related regulation can be brought into a more cohesive national privacy framework.

The ABA would be pleased to provide further assistance to the Committee if necessary.

Yours sincerely

_____

**Steven Münchenberg**