The Association of Superannuation Funds of Australia Limited
ABN 29 002 786 290
ASFA Secretariat
PO Box 1485, Sydney NSW 2001
p: 02 9264 9300 (1800 812 798 outside Sydney)
f: 1300 926 484
w: www.superannuation.asn.au

File Name: 2013/42

21 October 2013

Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001

Email: consultation@oaic.gov.au

Dear Commissioner,

Draft Australian Privacy Principles (APP) Guidelines – second tranche

The Association of Superannuation Funds of Australia (ASFA) is pleased to provide this submission in response to the second tranche of the draft *Australian Privacy Principle Guidelines*, covering the Australian Privacy Principles ("APPs") 6 to 11 ("the draft Guidelines").

ABOUT ASFA

ASFA is a non-profit, non-political national organisation whose mission is to protect, promote and advance the interests of Australia's superannuation funds, their trustees and their members. We focus on the issues that affect the entire superannuation industry. Our membership, which includes corporate, public sector, industry and retail superannuation funds, plus self-managed superannuation funds (SMSFs) and small APRA funds through its service provider membership, represent over 90% of the 12 million Australians with superannuation.

1. GENERAL COMMENTS

We have reviewed the draft Guidelines primarily from the perspective of superannuation funds, who will be APP entities under the recent amendments to the *Privacy Act 1988* ("the Act"), and their members. The superannuation environment is highly regulated, with large volumes of personal information required (directly or indirectly) by law to be collected, used and disclosed as part of the administration of members' superannuation monies. However, while the focus of our submission is on the particular impacts of the draft Guidelines on the superannuation industry, many of our comments will also apply to other sectors within the financial services industry.

As with tranche 1, we consider that the draft Guidelines provide clear and useful guidance for organisations as they move toward compliance with the privacy reforms. We again recommend that every effort is made to finalise and publish the Guidelines as soon as possible. We note that there are now less than five months until the commencement of the reforms, with consultation on tranche 3 of the draft Guidelines yet to commence.

Recommendation 1:
That the Commissioner releases the outstanding tranche of the draft Guidelines as soon as possible, and publishes the final Guidelines well before 12 March 2014.

We welcome the use of examples to emphasise the points made in the draft Guidelines. However, the lack of examples using scenarios relating to the provision of financial services is regrettable.

Given the volume of personal information handled by financial services entities, and the highly regulated environment in which those services are provided, we submit that there would be value in including some specific examples of how the APPs apply in the context of the relationship between an APP entity that is a financial services provider and the individual to whom such services are provided.

> **Recommendation 2:**
> That the Commissioner includes in the Guidelines examples of how the APPs apply in the context of the provision of financial services by an APP entity to an individual.

We note the OAIC's comment that it has further developed its interpretation of 'use' and disclosure' since the initial release of the 'key concepts' material in Chapter B (released as part of tranche 1 of the draft Guidelines). In this submission, we have accordingly limited any references to Chapter B to aspects which are, in our view, consistent with comments made in tranche 2, unless specifically noted.

2. SPECIFIC COMMENTS

Whilst ASFA broadly welcomes the recent amendments to the Act, we do have some concerns in relation to specific aspects of the draft Guidelines. These are set out below.

2.1. Chapter 6 – APP 6 – use or disclosure of personal information

2.1.1 Paragraph 6.8 – 'use'

The draft Guidelines provide significantly more guidance on the concepts of 'use' and 'disclosure' than the current *Guidelines to the National Privacy Principles*, and this generally will be welcomed by APP entities.

Paragraph B.108 states that an "an APP entity uses personal information when it handles and manages that information within the entity". Paragraph 6.8 (released as part of tranche 2) states that an APP entity 'uses' information "where personal information is handled, or an activity is undertaken with the information within the entity".

Paragraph 6.8 lists a number of examples of when an APP entity may be said to 'use' personal information'. In most cases these are common-sense examples which involve the entity taking some specific action in relation to the information – for example accessing and reading it, or making a decision based on it. However, the example given in the second bullet point in paragraph 6.8 (with similar wording used in paragraph B.108) - "searching records that contain the information" – has the potential to be interpreted in a manner which is, in our view, overly wide in scope.

In particular, the example could be taken to imply that merely searching *across* or *within* a record which happens to contain a specific item of information, without actively searching *for* that specific item, constitutes use of that item of information. If that is the case, it suggests that an entity could be taken to have 'used' *every item* of personal information contained within a record each and every time it searches that record, despite using specific search criteria to locate a particular item of information within an electronic record, or actively confining itself to searching for a particular item of information within a paper record. We submit that this cannot be the intended outcome.

To illustrate our concerns, consider the situation of an APP entity that provides ongoing financial services for an individual (the member), and maintains a record of personal information that has been collected for the purpose of administering the member's account and providing those services. The relationship between a financial services provider and member will typically span many years, and over this time a range of personal information may be collected by the entity and held as part of their record, often in an electronic format. From time to time, the entity will need to access the member's record, and certain items of information may be used and/or disclosed for a variety of reasons related to administration of their account – for example, responding to queries, providing periodic statements, calculating and paying benefit entitlements, reporting to regulators, etc.

Suppose the member in our scenario asks the entity for an estimate of their benefit entitlements (a routine type of enquiry). As this will depend on factors including the member's account balance and age, the entity accesses the member's electronic record and checks the member's date of birth. Applying the example in the second bullet point in paragraph 6.8 to this scenario, is the entity taken to have also 'used' every item of personal information in the member's record, including sensitive information?

If that is the intended interpretation, it will have severe and – in our view – unreasonably onerous consequences for APP entities, given the restrictive nature of many of the APPs. For example, where the member's records also contain copies of proof of identity documents which include a government identifier, the APP entity might be taken to have 'used' the identifier for a purpose which is not one of the permitted purposes within APP 9.2, even though it has not actively searched for that identifier nor undertaken any activity with it. (Please see 2.4.2 below for more detail about the particular need within the financial services industry to collect and retain proof of identity documents which might contain government related identifiers.)

> **Recommendation 3:**
> That the Commissioner clarifies the example of 'use' given in the second bullet point in paragraph 6.8. In particular, that the Commissioner confirms that simply accessing and/or searching within a record that contains an item of personal information does not automatically result in the 'use' of every item of information contained in that record. This could possibly be achieved by re-wording the second bullet point along the lines of "searching records for the information".

2.1.2 Paragraph 6.25 – relationship between the primary and secondary purpose

The third bullet point in paragraph 6.25 outlines a scenario where an individual's contact details, collected by an APP entity for the primary purpose of providing the individual with a subscription service, are used to notify the individual of a change in the APP entity's address. This is said to be a use of the individual's contact details for a secondary purpose, albeit one that is related to the primary purpose of providing the subscription service and that would be within the individual's reasonable expectations.

In our view, the use of an individual's contact details to notify them of the change of address of an entity that is providing them with a contracted service would not be a secondary purpose, rather it would be within the primary purpose of collection of the information. That is, most organisations – and, we submit, most individuals – would consider keeping an individual updated on any changes to the service provider's contact details to be 'part and parcel' of the provision of the underlying service, as it merely provides information that might be relevant to the individual in managing their subscription.

Classifying it as a 'secondary' purpose, albeit one that is related to the primary purpose, does not fully reflect the nature of the business relationship and requires an artificial and unnecessary analysis of the APP entity's purpose for the collection, use and/or disclosure of the information in question.

> **Recommendation 4:**
> That the Commissioner replaces the third example in paragraph 6.25 with one more clearly distinguishing between an APP entity's primary and secondary purpose.

2.2 Chapter 7 – APP 7 – direct marketing

2.2.1 Paragraph 7.8

Paragraph 7.8 notes that APP 7 does not apply to the use or disclosure of personal information to the extent that the *Do Not Call Register Act 2006* ("DNCR Act"), the *Spam Act 2003* ("Spam Act"), or any other prescribed legislation applies. We note that APP 7 will continue to apply to an APP entity to the extent that the activities or organisation in question is exempt from the DNCR Act, the Spam Act, or other relevant prescribed legislation. That is, the mere fact that the marketing activity involves telecommunications or a form of electronic communication that would ordinarily be covered by legislation other than the Act does not automatically mean that it will fall outside APP 7. We submit that it would be prudent to include a specific comment to this effect in the Guidelines.

Recommendation 5:
That the Commissioner includes a comment in the Guidelines acknowledging that APP 7 will continue to apply to direct marketing involving telecommunications and electronic communication methods governed by the DNCR Act and the Spam Act, where an exemption applies under those Acts.

We note that the OAIC currently provides more detailed guidance on the interaction between the Act and the Spam Act, as it applies in the context of the NPPs, in *Information Sheet 26*. This Information Sheet has provided valuable assistance for organisations in relation to their obligations under those Acts. We submit that additional guidance on these matters will continue to be necessary once the privacy reforms commence on 14 March 2014. Extension of the guidance to cover the DNCR Act would also be welcome.

Recommendation 6:
That the Commissioner updates the guidance currently contained in *Information Sheet 26 – interaction between the Privacy Act and the Spam Act* to:

- Reflect the amendments to the *Act* and the replacement of the NPPs with the APPs; and
- Cover the interaction between the Act and the DNCR Act.

2.2.2 Paragraph 7.12 – what is direct marketing?

Paragraph 7.12 notes that marketing is not 'direct marketing' if personal information is not used or disclosed, for example where an organisation sends catalogues by mail addressed 'To the householder'.

The conclusion that such activities are not 'direct marketing' is readily apparent in situations where the organisation engages in 'saturation marketing' and, for example, mails a catalogue to all mailing addresses in a particular location, without attempting to target particular recipients. However, were the organisation to use personal information to identify and target particular recipients, albeit physically addressing the catalogues 'to the householder' rather than to a named individual, this would appear to constitute 'use' of personal information. In such cases, it would appear that the organisation has therefore engaged in direct marketing.

Recommendation 7:
That the Commissioner redrafts the example in the first bullet point in paragraph 7.12, to more clearly show the distinction between activities that are 'direct marketing' and those that are not.

2.2.3 Paragraphs 7.15 – 7.19 – 'reasonably expects'

While paragraphs 7.15 – 7.19 provide helpful guidance for APP entities in assessing when an individual might reasonably expect their personal information to be used for direct marketing purposes, both of the examples provided (paragraph 7.17 and 7.19) are negative in nature. That is, they are examples of situations when an individual would *not* be said to have 'reasonable expectations'.

It would be helpful if the Guidelines also included at least one positively framed example – that is, an example of a scenario where an APP entity could conclude that an individual would reasonably expect their personal information to be used for direct marketing purposes.

Recommendation 8:
That the Commissioner includes in the Guidelines a positively framed example indicating when an APP entity might consider that an individual would reasonably expect their personal information to be used for direct marketing.

2.3 Chapter 8 – APP 8 – cross-border disclosure of personal information

2.3.1 Paragraphs 8.9 and 8.12 - the use of servers located outside Australia and cloud computing services

APP 8 is limited in scope to the 'disclosure' of personal information to an overseas recipient, it does not apply to the 'use' of that information (although other aspects of the APPs will apply in that instance).

Chapter 8 of the draft Guidelines includes examples which clarify the distinction between 'use' and 'disclosure' in the context of an APP entity routing personal information through servers located outside Australia (third bullet point in paragraph 8.8) and provision of personal information to a cloud service provider located overseas for the limited purpose of storing and managing personal information (paragraph 8.12).

In our submission on tranche 1 of the draft Guidelines, we noted the heightened level of due diligence required by APP entities in order to identify, and notify to individuals, the countries to which personal information may be disclosed 'through the cloud' (see recommendations 8 and 11 in that submission). As a result, we welcome the inclusion of examples specifically addressing the use of cloud services as well as servers located overseas.

We do, however, have these comments to make in relation to inclusion of these examples:

1. Given the stringency of the conditions in the example in paragraph 8.12, it is implicit that there will be cases where use of a cloud services provider may still involve a 'disclosure' of personal information. It would be helpful if this could be more explicitly stated in the Guidelines.
2. It is not clear whether the inclusion of the examples is part of the 'development' that has occurred in relation to the Commissioner's interpretation of 'use' and 'disclosure' since the publication of tranche 1 of the draft Guidelines. In any event, the approach applied to cloud computing services and offshore servers in paragraphs 8.8 and 8.12) should be reflected in the following sections of the final Guidelines (noting that the paragraph references below are from tranche 1):
    - Paragraph B.50, re the meaning of 'disclosure';
    - Paragraphs B.107 – B.109, re the meaning of 'use';
    - Paragraphs 1.25 – 1.28, re stating in the privacy policy the likely overseas disclosures; and
    - Paragraphs 5.24 – 5.28, re notifying individuals, when collecting personal information, about any likely cross-border disclosure.

In addition, we maintain our view that additional, more specific guidance on the privacy implications of using cloud computing services would be beneficial.

Recommendation 9:
That the Commissioner:

- Addresses more specifically the circumstances in which use of cloud computing services might constitute a 'disclosure' rather than a 'use' of personal information;
- Ensures, when finalising the Guidelines, that there is consistency between the views expressed in paragraphs 8.8 and 8.12 and chapters B, 1 and 5 (as noted above); and
- Considers providing specific guidance on compliance with the APPs, and in particular APP 8, for APP entities who utilise cloud computing services.

2.3.2 Paragraphs 8.14 – 8.16 – when will an APP entity have taken reasonable steps?

APP 8.1 provides that an APP entity must not disclose personal information to an overseas recipient unless it has taken 'reasonable steps' to ensure that the recipient does not breach the APPs in relation to that information.

Notwithstanding the taking of 'reasonable steps', section 16C provides that the APP entity will be accountable for any act or practice of the overseas recipient that would breach the APPs (subject to some exceptions). We note that this is a severe outcome, but one that results from the wording of the Act itself and not the drafting of the Guidelines.

Paragraph 8.14 of the draft Guidelines lists a number of circumstances that are relevant to determining the appropriate 'reasonable steps' for an APP entity – in effect, these outline a risk assessment process. Paragraph 8.15 then states:

> It is generally expected that an APP entity should enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the personal information in accordance with the APPs (other than APP 1).

While the use of the phrase "generally expected" suggests that an enforceable contract is an example of taking 'reasonable steps', the draft Guidelines do not provide any other examples. This tends to suggest that an enforceable contract is effectively a pre-condition for a cross-border disclosure, rather than simply one means of satisfying the 'reasonable steps' test.

Whilst it is not be unreasonable to expect a binding contract to be in place, we note that it is not an explicit requirement of APP 8.1 itself, and it does appear to be somewhat at odds with the risk based approach outlined in paragraph 8.14.

We recommend that the Commissioner clarify the 'expectation' that an APP entity will enter into a binding contract with an overseas recipient, and also provide examples of other types of actions which might constitute the taking of 'reasonable steps' to ensure that the overseas recipient does not breach the APPs.

> **Recommendation 10:**
> That the Commissioner reviews paragraphs 8.14 and 8.15 to clarify the expectation that a binding contractual arrangement will be in place between the APP entity and the overseas recipient, and provide examples of other 'reasonable steps' that can be taken by an APP entity to ensure that the overseas recipient complies with the APPs.

2.3.3 Paragraphs 8.17 – 8.25 – disclosure of personal information to an overseas recipient that is subject to a similar law or binding scheme

APP 8.2 provides that an APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the entity reasonably believes that the overseas recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is (overall) at least substantially similar to the way the APPs protect the information, and there are mechanisms that can be accessed by the individual to enforce that protection.

While paragraphs 8.20 – 8.24 of the draft Guidelines provides some general elaboration on APP 8.2, it is left to APP entities to make their own judgment about the 'similarity' or otherwise of the overseas law/scheme and the availability of mechanisms to enforce privacy protections.

Given the increasing globalisation of the commercial world, it is likely that an APP entity may, over time, have dealings with organisations based in a number of overseas jurisdictions. In many cases, an entity which was considering entering into an arrangement which might potentially have involved a cross-border disclosure of personal information may decide not to proceed after receiving preliminary legal advice indicating that the privacy protections of the jurisdiction in question are not 'substantially similar' to those provided by the APPs. Obtaining independent legal advice to assess the privacy protections afforded in the relevant jurisdiction(s), even on a preliminary basis, is likely to be both costly and time consuming for the APP entity.

We appreciate that it is not feasible for the OAIC to provide a full assessment of the privacy protections offered by all overseas jurisdictions. However, we consider that there would be significant value in the Commissioner providing, on the OAIC website, at least a 'baseline' level of information regarding the privacy protections afforded in key overseas jurisdictions, and extending the coverage progressively over time. At a minimum, this could:

- Identify any privacy or data protection law, or other law that imposes obligations on the handling of personal information, that applies in the jurisdiction;
- Address, at a high level, the 'factors' identified in paragraph 8.23 of the draft Guidelines in relation to assessing 'substantial similarity' between the APPs and the privacy protections afforded in the overseas jurisdiction; and
- Identify the mechanisms to enforce privacy protections that might apply in the overseas jurisdiction.

Provision of even high level information of this nature would help to educate APP entities about the privacy protections afforded in overseas jurisdictions, help make them informed decisions about potential cross-border disclosures of personal information, and assist them with compliance with APP 8.

We submit that the OAIC would already have access to this information for many jurisdictions, as the Commissioner would need to apply that knowledge in considering whether an organisation has complied with the current NPP 9 or, going forward, with APP 8.2.

Recommendation 11:
That the Commissioner considers providing, on the OAIC website, at least a baseline level of information about the privacy protections offered in overseas jurisdictions.

2.3.4 APP 8 and the impact of the Foreign Accounts Tax Compliance Act

Paragraphs 8.56 – 8.60 provide helpful guidance on the application of subsection 6A(4) to situations where an overseas recipient of personal information is required to disclose that information in order to comply with and applicable law in a foreign country. We note that the 'exemption' provided by subsection 6A(4) applies only to an act that is done, or a practice that is engaged in, outside Australia. As a result, it would not apply to a disclosure of personal information by an APP entity within Australia to an overseas recipient that is done in order to comply with an applicable law in a foreign country.

This raises particular concerns for the financial services industry, in the contest of compliance with the United States *Foreign Accounts Tax Compliance Act* ("FATCA"). Under FATCA, an Australian entity that is a Foreign Financial Institution ("FFI") may be required to disclose personal information in relation to certain of its customers/members to the Internal Revenue Service ("IRS"), in order to avoid incurring punitive withholding tax on its United States investments.

There are still a number of areas of uncertainty for Australian-based FFIs in relation to FATCA, and many financial services organisations are still determining whether they are 'deemed compliant' (effectively exempt) under the final FATCA regulations.

In addition, we note that the Australian and United States governments are currently negotiating an intergovernmental agreement. If finalised, this agreement would have the effect of streamlining any required disclosures of information, allowing non-exempt FFIs to report the prescribed information to the Australian Taxation Office ("ATO"), with the ATO in turn disclosing it to the IRS. As the intergovernmental agreement will be given effect to via Australian legislation, the disclosure by the Australian based FFI (the APP entity) to the ATO would be permitted under APP 6.2(b). The disclosure by the ATO to the IRS would be permitted under APP 8.2(e).

However, in the event that finalisation of the IGA is delayed, such that APP entities are required to begin reporting information directly to the IRS under FATCA, this would appear to involve cross-border disclosure of personal information in breach of APP 8.

Given the significance of FATCA for APP entities that are FFIs, it would be helpful if the Guidelines referred specifically to it, and if the Commissioner could also provide more detailed guidance – perhaps by way of an information sheet – addressing the Australian privacy implications of compliance with FATCA.

Recommendation 12:
That the Commissioner:

- Includes in the final Guidelines a specific reference to FATCA; and
- Provides additional, more detailed guidance for APP entities about the interaction between FATCA and their privacy obligations under the Act.

2.4 Chapter 9 – APP 9 – Adoption, use or disclosure of government related identifiers

2.4.1 Paragraphs 9.42 – 9.46 – use or disclosure of a government related identifier to an enforcement body for enforcement related activities

We note the concept of 'government related identifier' introduced in the recent amendments to the Act specifically includes identifiers assigned by a State or Territory authority. As a result, it is substantially wider than the concept of 'identifiers' that applies under the current Act and the NPPs.

Under the Act as amended, a drivers' licence number will now be a 'government related identifier', and as such its use and disclosure will be restricted under APP 9. This has particular significance for the financial services industry, as a driver's licence is one of the most common forms of photographic identification provided by an individual for identification purposes. Indeed, the 'Know Your Client' rules under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* and the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)* specifically provide for the use of a driver's licence as a 'primary photographic identification document'. A passport issued by the Commonwealth is similarly treated as a 'primary photographic identification document' for AML-CTF purposes, and is also frequently provided as identification by an individual in relation to the provision of financial services.

The use of these identifiers as part of the AML-CTF 'Know Your Client' process would, in our view, clearly fall within the scope of APP 9.2(a), which permits use or disclosure of a government related identifier of an individual if it is reasonably necessary for the organisation to verify the individual's identity for the purposes of its activities or functions.

Reporting entities for AML-CTF purposes are also required to report certain information to the Australian Transaction Reports and Analysis Centre ("AUSTRAC") in the event of a 'suspicious matter' arising – for example, a 'suspicion' that an individual is not who they claim to be. AUSTRAC may then request further information from the entity in order to investigate the matter, including copies of any purported identification documents that were provided by the individual. We believe that the disclosure of personal information contained on those documents would be justified under APP 6.2.(e): "the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body". To the extent that there is also a use or disclosure of a government related identifier contained on the documents, we consider this would also be justified under APP 9.2(e): "the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body".

Given the significant obligations imposed on reporting entities under the AML-CTF regime, and the impact that these obligations have on an entity's handling of customers' personal information, we consider it appropriate for the Guidelines to contain more extensive reference to AUSTRAC and the interaction between the Act and the AML-CTF regime.

Recommendation 13:
That the Commissioner:

- Includes the Australian Transaction Reports and Analysis Centre (AUSTRAC) in the list of examples of Commonwealth enforcement bodies for the purposes of APP 9.2(e) in paragraph 9.44 of the Guidelines; and
- Considers including in the Guidelines a detailed example involving disclosure to AUSTRAC of personal information, including government related identifiers.

2.4.2 APP 9.2 – interaction with paragraphs 6.8 and B.108

Entities in the financial services sector may be obliged to provide copies of identification documents may arise in response to a request from AUSTRAC (as noted above) or another enforcement body, by virtue of court order or the legislation governing the relevant body. An entity may also approach an enforcement body on its own initiative, for example because it has detected what it suspects to be fraud or criminal activity, and this may also lead to the disclosure of personal information that may include government related identifiers.

The potential need to comply with such obligations is the primary reason that many financial sector organisations retain an intact copy of personal identification documents provided by individuals, and do not systematically remove any government identifier from their records.

While we believe that the use and/or disclosure of a government related identifier to an enforcement body in the above circumstances would clearly fall within the exception in APP 9.2(e), we are concerned that the restrictive wording of APP 9.2, when read with paragraphs 6.8 and B.108 of the draft Guidelines in relation to the meaning of 'use', may lead to unintended consequences in other contexts.

Paragraph B.108 (released as part of tranche 1) states that an "an APP entity uses personal information when it handles and manages that information within the entity". Paragraph 6.8 (released as part of tranche 2) states that an APP entity 'uses' information "where personal information is handled, or an activity is undertaken with the information within the entity". Paragraph B.108 goes on to give, as an example of 'use', accessing information in the entity's control to "search records containing personal information", while paragraph 6.8 lists the example of "searching records that contain the information".

As noted in 2.1.1 above, this expansive concept of 'use' is of concern, when considered in light of the restrictive drafting of many of the APPs. In the particular context of APP 9.2, the examples noted above could potentially be interpreted as meaning that a government related identifier is 'used' every time an APP entity accesses and searches records which contain that identifier, even though the entity does not actively use the identifier itself as a search term. If so, the entity would contravene APP 9.2 simply by conducting routine functions in relation to the management of the individual's record and – in the financial services context – by administering their account. We submit that this cannot be the intended outcome.

Recommendation 14:
That the Commissioner confirms that where a government related identifier, included in a paper or electronic copy of a document used for identification purposes, is retained as part of an individual's record held by an APP entity, the entity does not 'use' the identifier in contravention of APP 9.2 merely by accessing and searching within the individual's record.

* * * * *

I trust that the information contained in this submission is of value. If you have any queries or comments regarding the contents of our submission, please contact Senior Policy Adviser, Julia Stannard on (03) 9225 4027 or via e-mail jstannard@superannuation.asn.au.

Yours sincerely

Fiona Galbraith
Director, Policy