31 July 2012

Natalya Wells
Inquiry Secretary
Standing Committee on Social Policy and Legal Affairs
PO Box 6021
Parliament House
Canberra ACT 2601

By email: spla.reps@aph.gov.au

Dear Ms Wells,

RE: Privacy Amendment (Enhancing Privacy Protection) Bill 2012

Thank you for the opportunity to comment on the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (**the Bill**).

The Financial Services Council (FSC) represents Australia's retail and wholesale funds management businesses, superannuation funds, life insurers and financial advisory networks. The FSC has over 130 members who are responsible for investing $1.8 trillion on behalf of more than 11 million Australians.

The pool of funds under management is larger than Australia's GDP and the capitalisation of the Australian Stock Exchange and is the fourth largest pool of managed funds in the world. The FSC promotes best practice for the financial services industry by setting mandatory Standards for its members and providing Guidance Notes to assist in operational efficiency.

This submission is made on behalf of the FSC's life insurance Members.

The FSC is broadly supportive of the privacy legislation reforms proposed in the Bill. We note that the proposed reforms are 'technology-neutral' to encompass both traditional and modern methods of communication and storage of customer information. We consider that this is important due to the fact that the current Privacy Act 1988 (Cth) pre-dates a number of technological advances which are commonly used in 2012.

We note that the Bill provides a flexible, non-prescriptive approach which allows organisations to develop appropriate policies and procedures depending on their size, nature and industry to meet the Australian Privacy Principles and other obligations set out in the Bill. However, as a consequence of this flexible, non-prescriptive approach, we submit that there are a number of new obligations outlined in the Bill that are potentially ambiguous and therefore may lead to confusion in their application.

Our submission covers the following matters in relation to the Bill.

1. **General comment**
2. **Transition Period**
3. **Australian Privacy Principles - Prospective as opposed to retrospective**
4. **Australian Privacy Principles – Guidelines**
5. **APP7 – Direct Marketing**
6. **APP8 -Information flows within Organisations**
7. **APP8 – Computer Servers and Cloud Computing**
8. **Powers of the Office of the Australian Information Commissioner (OAIC) – General**
9. **Powers of the OAIC – Complaints**

Please contact me on [redacted] if you would like to discuss any aspect of this submission.

Yours sincerely

Holly Dorber
Senior Policy Manager

1. Transition Period

We note that in the Commencement section of the Bill the majority of new obligations are effective after a transition period which is cited as, *"The day after the end of the period of nine months beginning on the day this Act receives the Royal Assent."* FSC Members collectively hold personal and sensitive information about millions of customers. The nature of the life insurance industry is such that prospective customers are required to provide information including health and financial information to their insurers prior to commencement of the policy at the underwriting stage and during the assessment of a claim.

This information is contained within a vast range of soft and hard copy documents including correspondence, telephone records, computer systems, application and claim forms. For us to implement the requirements of the new Australian Privacy Principles we will need to carry out the following tasks:

a) Review how current information is collected, stored, used and disclosed;
b) Make relevant changes to our systems to comply with the new requirements;
c) Amend our customer facing documentation such as product disclosure statements, application forms, claims forms, insurance policy documents and websites;
d) Communicate the changes to our customers;
e) Undertake training for relevant staff dealing with customer information;
f) Reviewing and amending if necessary, our contracts with third parties relating to cross border arrangements; and
g) Amend our existing policies and procedures to implement the new obligations.

The lead time necessary to update our customer facing documentation and in particular, product disclosure statements, in respect of each life insurance product is considerable. Due to the complexity and time involved to implement these changes we strongly submit that a transition period of eighteen months is both appropriate and realistic for organisations to prepare for the new obligations.

2. Australian Privacy Principles - Prospective as opposed to retrospective

Organisations represented by the FSC are currently required to comply with the following National Privacy Principles:

- Principle 1 - Collection
- Principle 2 - Use and disclosure
- Principle 3 - Data quality
- Principle 4 - Data security
- Principle 5 - Openness
- Principle 6 - Access and correction
- Principle 7 - Identifiers
- Principle 8 - Anonymity
- Principle 9 - Transborder data flows
- Principle 10 - Sensitive information

We note that the new Australian Privacy Principles outlined in Schedule 1 of the Bill are intended to replace the National Privacy Principles from the end of the transition period. However, it is unclear from the terminology of the draft legislation whether the new principles listed below are intended to apply prospectively.

Australian Privacy Principle 1—open and transparent management of personal information

Australian Privacy Principle 2—anonymity and pseudonymity

Australian Privacy Principle 3—collection of solicited personal information

Australian Privacy Principle 4—dealing with unsolicited personal information

Australian Privacy Principle 5—notification of the collection of personal information

Australian Privacy Principle 6—use or disclosure of personal information

Australian Privacy Principle 7—direct marketing

Australian Privacy Principle 8—cross-border disclosure of personal information

Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

Australian Privacy Principle 10—quality of personal information

Australian Privacy Principle 11—security of personal information

Australian Privacy Principle 12—access to personal information

Australian Privacy Principle 13—correction of personal information

While those Australian Privacy Principles that relate to collecting and receiving information could be viewed as prospective in application, the position is not clear for those Principles that relate to the use (for example, under Australian Privacy Principle 7), disclosure (for example, under Australian Privacy Principle 8), obtaining of consents for use and disclosure (for example, under Australian Privacy Principle 7) and holding of information which was collected by organisations prior to the end of the transition period.

FSC life insurance Members hold enormous amounts of non-active customer information such as lapsed policies, underwriting applications that have not proceeded into an in-force policy, archived claim files and lost members. There would appear to be no public interest benefit for insurers to communicate their new privacy policies and procedures to previous or existing customers and/or applicants who have not proceeded with their policy or where the policy is out of force. The financial and administrative burden of contacting these categories of customers would not be justified and we strongly submit that the new APPs should apply only to customers from the relevant commencement date. For the avoidance of doubt we submit that it would be useful if the OAIC specified that the existing NPPs apply during the transition period.

3. Australian Privacy Principles – Guidelines

The expectations of the Privacy Commissioner regarding the National Privacy Principles were clearly articulated in the Guidelines published in September 2001. These are helpful for organisations in that

they set out the steps that should be taken to comply with the principles and this document is frequently used as a reference point by privacy specialists.

We respectfully submit that guidelines to the new Australian Privacy Principles should be published by the OAIC during the transition period to assist organisations with requirements and prevent confusion or ambiguity regarding wording of particular requirements within the principles.

4. Direct Marketing – APP7

In APP 7, the exemptions in paragraphs 7.2 to 7.4 stipulate different levels of restrictions on the use personal information or sensitive information for direct marketing. It appears to be the intention of the Australian Law Reform Commission that additional privacy controls would apply to direct marketing in its Report 108.

However:

a) the mention of the *Spam Act* and *Do Not Call Register Act* in paragraph 7.8 creates an ambiguity regarding whether APP 7 (not limited to paragraphs 7.2 to 7.4) will only apply to communications which are not caught under the *Spam Act* and *Do Not Call Register Act* (i.e. apply only to postal and facsimile communication, and not to emails, SMS, telephone calls);

b) in relation to paragraph 7.4, it appears that as long as consent is obtained from the individual for the use or disclosure of sensitive information for the purpose of direct marketing, there is no need to provide a means to opting out of receiving marketing materials, or have a prominent statement on the marketing materials regarding the ability to opt out.

Direct marketing is commonly used by life insurers (and their intermediaries). There is a compliance cost involved in making changes to systems that generate direct marketing and processes for monitoring the obtaining of consents. The FSC seeks clarity on the above issues in order to implement appropriate systems and processes to comply with APP7.

We submit that APP 7 and the Explanatory Memorandum be sufficiently clear on:

a) which aspects of APP 7 would and would not apply if the communication is caught under the Spam Act and Do Not Call Register Act;

b) whether the obligations under paragraph 7.4 in relation to sensitive information are in addition to those in paragraphs 7.2 and 7.3 (whichever applies to a communication); and

c) whether APP 7 is intended to apply prospectively for new customers or both prospectively for new customers and retrospectively for existing customers as mentioned above under section 2 (Australian Privacy Principles - Prospective as opposed to Retrospective),.

We would submit that the Australian Privacy Principles apply only prospectively in respect of personal information collected after the commencement date of the new changes and after an appropriate transition period.

5. APP8 -Information flows within organisations

The Life Insurance industry in Australia is well regulated and as such there are numerous existing regulations in place to ensure that customer information, which is often sensitive information, is protected and that policyholder interests are protected.

One feature of the Australian life insurance market is the presence of large multi-national entities in the Australian market. For those entities to provide efficient service to the Australian market they must be certain that they can disclose information within the organisation, including to related entities located overseas (provided that such disclosure is subject to reasonable controls with respect to privacy). We are concerned that the new APP8 imposes a significantly more onerous accountability provision that has the potential to impede the use of global services by providing that an entity will be liable for any acts done, or by practices engaged in by the overseas entity in relation to the personal information received.

A review of APP8, in particular in conjunction with the Explanatory Memorandum, does not provide sufficient clarity or comfort to those entities that the disclosure of information within a corporate group will be permitted. The Explanatory Memorandum provides that:

Although APP 8 explicitly adopts the term 'disclosure' rather than 'transfer', the APP 8 (and related provisions) would not apply to the overseas movement of personal information if that movement is an internal use by the entity, rather than a disclosure. APP 8 will apply where an organisation sends personal information to a 'related body corporate' located outside Australia.

The foregoing is not sufficiently precise to provide comfort to an industry that moves information within the organization to assist in the provision of services in Australia. By way of example, Life insurers may have their payment processing for claims located offshore and managed by a related body, APP8 needs to be clear that the provision of information between those related entities (always subject to reasonable controls) will be an exception to the new requirements imposed by AAP8.

Members of the life insurance industry increasingly look to use service providers that are located overseas to provide key services. These services are varied and include administrative as well as customer-facing services. This is a reflection of the globalisation of business and increasingly, an economic necessity to ensure that the life insurance industry remains competitive. We submit that it is vital that the Australian Privacy Principles such as APP8 do not unduly inhibit the convenient and increasingly necessary flow of information across borders.

Therefore, we submit that APP8 should be amended to include the exceptions relating to the performance of contracts that presently exist within NPP 9.1 (c) and (d):

> *The transfer is necessary for the performance of a contract between the individual and the organization or for the implementation of pre-contractual measures taken in response to the individual's request; and*
>
> *The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organization and a third party.*

Therefore, we further submit that APP 8 and the Explanatory Memorandum should be sufficiently clear to provide entities certainty that those entities will be able to transfer or disclose information between related corporate entities provided that there are measured and reasonable controls in place to ensure that the information which it has disclosed will not be held, used or disclosed by the recipient in a manner that is inconsistent with the APPs. This clarity is needed to ensure that Australian customers receive seamless service from all participants in the Australian life industry.

6. APP8 – Computer servers and cloud computing

We submit that the changes proposed in the Bill as a whole and the APPs generally should be 'technology-neutral' with an eye to future technological changes. With that in mind, we submit that the current and future use of Cloud storage systems for computer networks may cause unintentional breaches of APP8.

It should be noted that the life insurance industry is regulated by the Australian Prudential Regulation Authority (APRA) to ensure that when information is transferred overseas that those arrangements must be documented between the company and computer storage outsource entity and subject to Australian oversight.

It is our submission, that the entire Bill, including the APPs (and in particular, APP8), should be drafted in such a manner that any future changes to technology will not cause issues with respect to internal management of information and its potential overseas transfer. By way of example it is likely that cloud computing storage systems will become common if not normal practice in the next few years. APP8 must address the issue that future technology may make it impossible for a company or entity using a cloud system to be aware of the actual location of the information given that the nature of the technology.

We submit that APP8 should be drafted in such a manner that transfers within a closed computer storage system or network would not be deemed a disclosure with respect to APP8 or worse a breach of APP8.

7. Powers of the OAIC – General

As noted above, life insurers are in receipt of a vast amount of personal and sensitive information about policyholders which is required for them to provide their products and services. For example, medical records are often required at the underwriting and claims stage, with income details required for products such as income protection payment calculations. Both APRA and the Australian Securities and Investments Commission (ASIC) impose significant requirements on life insurers and holders of financial services licenses under their respective regulatory frameworks and both entities

have a substantial range of investigative and enforcement options. Section 93A of the ASIC Act 2001 and RG 100 provide details on enforceable undertakings. Similar provisions for APRA are contained in the APRA Act 1998 and the SIS Act 1993. In the experience of FSC Members, both ASIC and APRA carry out their regulatory functions in a consultative manner which has regard to due process, provides Members with the opportunity to make submissions and present information and materials to assist the regulator and explain the particular circumstances under investigation.

We submit that it would be appropriate for the OAIC to have regard to and adopt a similar approach and methodology of existing regulators such as APRA and ASIC when exercising the new regulatory powers.

8. Powers of the OAIC – Complaints

Section 41 of the Bill states that the commissioner "may or must" decide not to investigate etc. in certain circumstances including when the act or practice is being dealt with by an external dispute resolution scheme. The FSC submits that where a complaint is being handled by FOS or the SCT, it would be prudent if the OAIC should exercise its discretion to defer investigating the complaint until the conclusion of the FOS or SCT investigation.

Financial services providers are required under s912A Corporations Act 2001 to have a dispute resolution process for customers. For life insurance products held under superannuation, life insurers are obligated to have a stringent internal and external dispute resolution process with superannuation trustees obligated under S101 SIS Act to refer complaints to the Superannuation Complaints Tribunal in cases where the internal dispute resolution process has not provided a satisfactory outcome for the complainant. There is a similar process for retail life insurance products, with complaints having access to the Financial Ombudsman Scheme.

The Australian Financial Services License conditions stipulate that entities holding a license must have an internal and external dispute resolution process. The percentage of life insurance complaints involving alleged breaches of privacy rights is minimal compared to complaints about policy terms, claims payments, fees and similar issues..

In view of these existing avenues for dispute resolution, there is significant potential for there to be multiple complaints and proceedings in relation to the same or similar dispute. We submit that when considering its jurisdiction to analyse a complaint, the OAIC defer initiating any process in cases involving life insurance products where there are concurrent internal and/or external complaints resolution processes already underway and before these have been completed.

We note that the Bill states that:

> *In exercising the complaints powers it is expected that the Commissioner will:*
>
> - *apply the principles of administrative law;*
> - *outline, as appropriate, in the annual report, examples of where the power is used; and*

- *provide guidance as to the kinds of matters it would decline to investigate.*

Occasionally life insurers deal with circumstances where actual or suspected criminal activity has taken place such as the murder of a life insured by a named beneficiary, insurance fraud which may involve whistle-blower elements and other circumstances where it would be against public policy for the OAIC to investigate an alleged breach of privacy rights by the perpetrator of the offence.

We submit that consideration be given to redrafting the powers accordingly, or alternatively to address the public policy circumstance in the guidelines for the kinds of matters that the OAIC would decline to investigate.

We a;sp submit that the new proposed increased powers of the OAIC and sanctions for breaches of the APPS, will significantly deter any organisation from failing to take reasonable steps to ensure recipients use personal information about Australian individuals consistent with the APPs.