SENATE STANDING COMMITTEE ON FINANCE AND PUBLIC ADMINISTRATION

LEGISLATION COMMITTEE

Exposure Drafts of Australian Privacy Amendment Legislation

SUBMISSION

SUBMISSION NUMBER: **34**

SUBMITTER

Financial Services Council

FSC FINANCIAL SERVICES COUNCIL

18 August 2010

Senate Finance and Public Administration Committee
PO Box 6100
Parliament House
Canberra ACT 2600
Australia

By email: fpa.sen@aph.gov.au

Dear Sir/Madam

Australian Privacy Principles: Exposure Draft

The Financial Services Council[1] is the peak body representing the retail and wholesale funds management, superannuation and life insurance industries. The Financial Services Council has over 135 members who are responsible for investing over $1 trillion on behalf of more than ten million Australians.

We are grateful for the opportunity to make this submission on the Exposure Draft of the Australian Privacy Principles (APPs).

Before commenting on the APPs, we make the following general submissions concerning the Privacy regulatory framework, with key points concerning life insurance.

- The Financial Services Council (FSC) supports a single, federal legislative framework for Privacy, and the reduction of any overlap between federal and state laws.
- The collection of family medical information from an individual applying for life insurance is critical in enabling life insurers to assess risk. Any impediments arising from the APPs or other provisions of the Privacy regime with the collection of such information *from the applicant* would potentially increase the level of risk and in turn, the cost of insurance.
- Investigation and surveillance techniques employed by life insurers help to reduce fraudulent life insurance claims. Surveillance is an essential tool to identify fraud.
- The above points concerning life insurance are important because Australia has a chronic underinsurance problem.

We provide comments below on specific Principles.

[1] The Financial Services Council, until recently, was known as the Investment and Financial Services Association (IFSA).

Financial Services Council Ltd
ABN 82 080 744 163
Level 24, 44 Market St
Sydney NSW 2000
T. +61 2 9299 3022
F. +61 2 9299 3198
E. info@fsc.org.au
W. fsc.org.au

APP 5 (notification of the collection of personal information)

This Principle requires that entities take reasonable steps (if any) to notify or ensure the individual is aware of certain details before, at, or as soon as practicable after the collection of the information.

It would appear that this Principle imposes a continuous disclosure notification on entities. Arguably, the nature of certain relationships (such as the financial planning relationship) may make the continuous disclosure notifications unnecessary for existing clients after initial disclosure is made at the first meeting. Clarification of what is meant by "reasonable steps" via examples would be useful to ensure a consistent application of the requirements under this principle.

FSC also submits that notification to an individual may be by reference to information on an entity's website.

APP 6 (use or disclosure of personal information)

The exception relating to a reason to suspect unlawful activity is currently restricted to the entity's activities. This exception should be expanded to any situation where the entity reasonably suspects any kind of unlawful activity, for example fraud, money laundering or terrorism financing.

APP 7 (direct marketing)

APP 7 should clarify that organisations only need to reveal the source of the information from which they themselves received the individual's information, not the ultimate source of the information.

APP 7 (1)(a) requires that organisations must not use or disclose information for the purposes of direct marketing unless, for sensitive information, the individual has consented to the use or disclosure of the information for that purpose.

For non-sensitive personal information, there is a requirement under APP 7(2)(c) that an organisation must provide a simple means by which the individual may easily request not to receive direct marketing communications from the organisation.

The way APP 7 is drafted does not appear to afford an equivalent opt-out facility in relation to sensitive information. From a practical perspective, it is unclear how the consent requirement under APP 7(1)(a) would operate without an appropriate opt-out mechanism.

The FSC also suggests that further guidance is warranted concerning the following:

- what constitutes "consent" between companies in the same group, that is, is it sufficient to simply have an agreement that all information will be shared;

Financial Services Council Ltd
ABN 82 080 744 163
Level 24, 44 Market St
Sydney NSW 2000
T. +61 2 9299 3022
F. +61 2 9299 3198
E. info@fsc.org.au
W. fsc.org.au

- the types of direct marketing communications that are likely to be within the reasonable expectations of clients who have provided consent;
- the kinds of circumstances in which it will be impracticable for an organisation to seek consent in relation to direct marketing; and
- factors for an organisation to consider in determining whether it will be reasonable and practical to advise an individual of the source from which it acquired the individual's personal information.

APP 8 (cross-border disclosure of personal information)

While it is not apparent from a reading of APP 8 itself, section 19 of the Exposure Draft (Extra-territorial operation of this Act) appears to apply the APPs to an overseas customer of an entity that operates in Australia. For example, an Australian life company operating in and collecting information from New Zealand insurance applicants in New Zealand appears to be subject to the APPs, including the requirements to notify of the collection of the information (APP 5). The Australian life company will also be subject to New Zealand privacy requirements in relation to information collected in NZ. This duplication needs to be prevented by limiting the APPs to information collected in Australia. To be clear, the APPs should apply to information collected in Australia and transferred overseas, but not to information collected overseas by an entity that operates in Australia.

On the matter of offshore transfer of data, the Companion Guide states that it is not intended that personal information will have been "disclosed" simply because it has been routed through servers outside Australia. For the avoidance of doubt, the FSC submits that this matter should be clarified in APP 8, and in supporting provisions of the Privacy Act. It should also be made clear that the offshore storage of data (where the storage provider does not have access to the data) also does not constitute "disclosure" of personal information.

APP 11 (Security of personal information)

APP 11 requires an entity to take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure.

Further guidance should be provided on aspects of this Principle to ensure clarity, including:

- when it is appropriate to destroy or render non-identifiable personal information, including personal information that forms part of a historical record and may need to be preserved, in some form, for the purpose of future dispute resolution;
- the interaction between data destruction requirements and legislative record retention requirements.

Clarification in relation to these two points is essential, as standard practice within the financial services industry is to maintain records for 7 or 10 years after the last date of the interaction with the client. To ensure that all legislative requirements can be appropriately complied with, the requirement to destroy or de-identify under APP 11 should commence

Financial Services Council Ltd
ABN 82 080 744 163
Level 24, 44 Market St
Sydney NSW 2000
T. +61 2 9299 3022
F. +61 2 9299 3198
E. info@fsc.org.au
W. fsc.org.au

after other legal requirements for record retention timeframes have been met.

APP 13 (correction of personal information)

The extent of the proposed obligation for an entity to take reasonable steps (if any) to notify a correction to third parties is unclear. For example, in order to meet this obligation, must entities meet a request from an individual to notify third parties of corrected personal information by tracking and recording all third parties to whom the client's personal information has been provided to, as well as all the particular personal information disclosures we make to these other parties? If so, this proposal would create a particularly onerous administrative burden on FSC members, and is likely to result in significant compliance costs for the financial services industry.

Further, the obligation to correct should only be triggered by the request of the individual. This ensures that the individual has confirmed that information is inaccurate and should be amended or deleted.

General comments

The FSC submits that any reforms to the current Privacy regime should be applied prospectively and with an appropriate transition period. For FSC members, this would facilitate the necessary systems changes and any adjustments to customer communications that may be necessary.

The FSC also submits that a revised Privacy regime must be aligned, where appropriate with other regulatory regimes such as the *Corporations Act,* the *AML/CTF Act*, and taxation laws. Specific requirements in these and other laws to collect, use and disclose information should take precedence over the Privacy regime.

Finally, where we have suggested that further guidance be provided in relation to the APPs, and indeed any aspect of the Privacy regime, members of the FSC would be pleased to work with government and the Office of the Privacy Commissioner to develop such guidance.

Please contact me on (02) 8235 2531 if you wish to discuss these matters further.

Yours sincerely

Vicki Mullen
Senior Policy Manager

Financial Services Council Ltd
ABN 82 080 744 163
Level 24, 44 Market St
Sydney NSW 2000
T. +61 2 9299 3022
F. +61 2 9299 3198
E. info@fsc.org.au
W. fsc.org.au