Law Council
OF AUSTRALIA

11 July 2012

Ms Natalya Wells
Inquiry Secretary
Standing Committee on Social Policy and Legal Affairs
Department of the House of Representatives
PO Box 6021
Parliament House
Canberra ACT 2600

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

Dear Ms Wells

INQUIRY INTO THE PRIVACY AMENDMENT (ENHANCING PRIVACY PROTECTION) BILL 2012

Thank you for your invitation of 10 July 2012 to make a submission to the inquiry into the Privacy Amendment (Enhancing Privacy Protection) Bill 2012.

I enclose a submission which was prepared by the Privacy Law Committee of the Business Law Section of the Law Council of Australia and submitted to the Senate Standing Committee on Legal and Constitutional Affairs. Owing to time constraints for providing submissions to this inquiry, the submission has not been reviewed by the Directors of the Law Council.

If you have any questions in relation to the submission, in the first instance please contact the Chair of the Privacy Law Committee, [redacted]

Yours sincerely

[redacted]

Professor Sally Walker
Secretary-General

Attachment: Submission

GPO Box 1989, Canberra
ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612

Telephone **+61 2 6246 3788**
Facsimile +61 2 6248 0639

Law Council of Australia Limited
ABN 85 005 260 622
www.lawcouncil.asn.au

Law Council
OF AUSTRALIA

Privacy Amendment (Enhancing Privacy Protection) Bill 2012

Senate Standing Committee on Legal and Constitutional Affairs

11 July 2012

GPO Box 1989, Canberra
ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612

Telephone **+61 2 6246 3788**
Facsimile +61 2 6248 0639

Law Council of Australia Limited
ABN 85 005 260 622
www.lawcouncil.asn.au

Table of Contents

Introduction

The Law Council of Australia is pleased to provide this submission in response to the Senate Standing Committee on Legal and Constitutional Affairs' inquiry into the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (the Bill).

As outlined in Attachment A, the Law Council represents the Australian legal profession through the bar associations and law societies of each State and Territory and the Large Law Firm Group (the '"constituent bodies' of the Law Council). The Law Council also has a number of specialist sections consisting of individual members of the legal profession with particular interest in specific areas of law, such as business law.

This submission has been prepared with input from the Privacy Law Committee (the Committee) of the Business Law Section of the Law Council.

The Law Council refers the Senate Standing Committee to the submissions it has previously made on iterations of parts of the Bill, including:

- Submission to the Senate Finance and Public Administration Committee inquiry into the Australian Privacy Principles Exposure Draft, dated 17 August 2010 (First Submission); and
- Submission to the Senate Finance and Public Administration Committee inquiry into the Australian Privacy Principles Exposure Draft, dated 25 March 2011 (Second Submission).

The Law Council understands that two of its constituent bodies, the Law Institute of Victoria and the Queensland Law Society, have provided submissions to the inquiry and the Law Council directs the Senate Standing Committee to these submissions.

The Law Council may wish to provide further comment if there is an opportunity to do so at any subsequent stages of this inquiry.

Part A - Australian Privacy Principles (APPs)

Structure and drafting of the APPs

The Bill amends the *Privacy Act 1988* (Privacy Act) to create the APPs, a single set of privacy principles applying to both Commonwealth agencies and private sector organisations. The APPs replace the public sector Information Privacy Principles (IPPs) and the private sector National Privacy Principles (NPPs).

As set out in the First and Second Submissions, the Committee submits that the simple language and structure contained in the current NPPs has been replaced with a more verbose and complex set of principles.

The Committee submits that the structure and drafting of the APPs should be reviewed with the aim of reverting to the simpler drafting style of the NPPs. That structure and language is based on and referable to the original Organisation for Economic Co-operation and Development (OECD) Guidelines for the Protection of Privacy and Transborder Flows of Personal Data[1] which have been used as the basis for relevant provisions at state and territory and international levels. The Committee considers that

[1] See http://www.oecd.org/document/18/0,3746,en_2649_34223_1815186_1_1_1_1,00.html.

the proposed APPs are difficult to interpret and therefore less accessible to privacy practitioners, regulated organisations, consumers and ordinary members of the public.

Similar comments have been made by others, including the Senate Finance and Public Administration Committee in its May 2012 report on the Exposure Drafts of Australian Privacy Amendment Legislation: Part 1 – Australian Privacy Principles.

Accordingly, the Committee suggests that the Senate Standing Committee should recommend that the drafting of the APPs should be reviewed with the aim of simplification and concision.

The Second Submission provides several suggestions for how the drafting might be reviewed, including the following example. APP 2 currently provides:

> *Australian Privacy Principle 2 – anonymity and pseudonymity*
>
> 1) *Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.*
> 2) *Subsection (1) does not apply if:*
>   a. *the APP entity is required or authorised by or under an Australian law, or court/tribunal order, to deal with individuals who have identified themselves; or*
>   b. *it is impracticable for the APP entity to deal with individuals who have not identified themselves.*

This replaces NPP 8, which provides:

> *Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.*

As the meaning remains essentially unchanged, the Committee submits that the wording of NPP 8 should be preferred and applied to APP entities, namely agencies and organisations.

Introductory remarks relating to the distinction between 'agencies' and 'organisations'

As noted above, the Bill amends the Privacy Act to create the APPs, a single set of privacy principles applying to both agencies and organisations. However, the Bill retains a distinction between 'agencies' and 'organisations' in the application of some of its provisions. While the Committee understands this is necessary in some contexts, it views some of these distinctions as unnecessary and undesirable.

Section 7A - application of provisions in APPs relating to organisations in respect of the commercial activities of agencies

The Committee has concerns regarding the way in which agencies regulated by the *Commonwealth Authorities and Companies Act 1997* (Cth) (CAC Act) are affected by the operation of some APPs when considered in the context of section 7A of the Privacy Act.

Section 7A provides that the Privacy Act applies to the acts and practices of certain agencies in respect of their commercial activities, as if the agencies were organisations. This section remains unchanged by the Bill and affects a number of CAC Act agencies including the Australian Broadcasting Corporation (ABC), Special Broadcasting Service

(SBS), Australia Post, the Commonwealth Scientific and Industrial Research Organisation (CSIRO), Comcare and the Reserve Bank of Australia.

Some of the distinctions between agencies and organisations in the Privacy Act (as amended by the Bill) apply at the entity level, for example, the exemption from the protections of the Privacy Act for employee records applies only to organisations. Where that is the case, section 7A has no application.

The Explanatory Memorandum to the Bill (EM) and the notes in the APPs suggest there is a continued need for section 7A in relation to APP 7 (relating to direct marketing) and APP 9 (relating to the use of government identifiers), as APP 7 and APP 9 as drafted apply only to 'organisations'. Relevant CAC Act agencies will need to comply with APPs 7 and 9 in relation to their commercial activities as a result of the application of Section 7A.

If section 7A remains unchanged while these distinctions remain, then relevant agencies will still have to establish and monitor two sets of rules for different parts of their business. This outcome is contrary to the stated objectives that the same principles apply in so far as possible to agencies and organisations.

Sharing between related bodies corporate

Section 13B permits sharing between related bodies corporate, however s13B(1)(a) provides than an organisation cannot share with an entity that is not an organisation.

No substantive amendments have been made to this provision. As both agencies and organisations are to be subject to a single set of principles, the Committee submits that related entities should be able to take advantage of this permitted sharing of information irrespective of whether they are agencies or organisations.

In addition, the Committee submits that APP 6.6 seems to overlook this qualification on the basis that all APP entities collecting personal information from a related body corporate have the benefit of, and will share under, that provision.

APP 6.1 provides that an APP entity which holds personal information about an individual that was collected for a particular purpose (the primary purpose) must not use or disclose the information for another purpose (the secondary purpose) except in certain circumstances. Personal information is defined in the Privacy Act as 'information or an opinion …about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion'.

APP 6.6 provides that if an APP entity is a body corporate and collects personal information from a related body corporate, the non-disclosure principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Overseas act required by foreign law

The Bill proposes to amend section 6A of the Privacy Act which relates to breaches of NPPs by replacing the references to NPPs with references to APPs. However, sub-sections (2) and (3) of section 6A currently refer only to acts or practices of organisations which do not breach NPPs. Sub-section (4) provides that an act or practice does not breach a NPP if it occurs outside Australia and is required by an applicable law of a foreign country. This sub-section will be amended to refer to the APPs and therefore extend to agencies.

Section 13D provides that an act or practice of an organisation done or engaged in outside Australia is not an interference with the privacy of an individual if it is required by an applicable law of a foreign country. This section is not proposed to be amended by the Bill.

The Committee believes it is unnecessary to include both sections 6A(4) and 13D as the two provisions essentially operate under the same terms. If both provisions are included, it is submitted that section 13D should be extended to apply to agencies.

Collection of solicited personal information

The Committee does not understand the reasoning behind the two different tests under APPs 3.1 and 3.2.

Under APP 3.1, an agency must not collect personal information unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

Under APP 3.2, an organisation must not collect personal information unless the information is reasonably necessary for one or more of the organisation's functions or activities.

The EM provides that the additional words in APP 3.1 reflect the test in the current IPP 1 and are necessary because "… there may be agencies that need to collect solicited personal information in order to carry out legitimate and defined activities, but may not be able to meet the 'reasonably necessary' test. While the 'directly related to' test may … be a slightly lower threshold, agencies are subject to a wider range of accountability mechanisms …".[2]

The Committee does not see how it can be reasonably necessary for one or more of an agency's functions or activities to collect personal information (other than sensitive information) without that collection also being directly related to that agency's functions or activities. Accordingly, and for the sake of drafting simplicity, the Committee suggests that APP 3.1 and 3.2 be condensed into one provision, omitting the words "or directly related to".

Moreover, the Committee is uncertain of the operation of section 7A in relation to APPs 3.1 and 3.2, which are drafted in such a way that it appears that APP 3.1 will apply to all activities of an agency and APP 3.2 will apply to all activities of an organisation. If APP 3.1 read "An agency must not …" and APP 3.2 read "An organisation must not …" then Section 7A could arguably operate to apply APP 3.2 to the commercial activities of an agency. The Committee reiterates its position that one provision should apply to all APP entities. If APPs 3.1 and 3.2 remain as drafted, it should be expressly stated that section 7A has no application to these APPs.

The Committee submits that these comments apply also to APPs 3.3(a)(i) and 3.3(a)(ii), which relate to the prohibition of the collection of sensitive information about individuals without consent and unless the information is 'reasonably necessary for, or directly related to, one or more of the agency's functions' or 'reasonably necessary for one or more of the organisation's functions'. Sensitive information is defined in the Privacy Act as particular forms of personal information such as religious beliefs; health information and genetic

[2] See Explanatory Memorandum available at http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4813_ems_00948d06-092b-447e-9191-5706fdfa0728/upload_pdf/368711.pdf;fileType=application%2Fpdf at p 75.

information. Health information is personal information relating to health or disability, health services, organ donation and certain genetic information.[3]

The Committee submits that APPs 3.3(a)(i) and 3.3(a)(ii) should be combined into one provision omitting the words "or directly related to".

Use or disclosure of personal information when a permitted health situation exists

The Committee submits that APP 6.2(d), relating to use or disclosure of personal information in the case of a permitted health situation, should also apply to agencies. A permitted health situation is defined in proposed section 16B allowing the collection by an organisation of health information about an individual in certain situations.

Exceptions to access

APP 12.1 provides that if an APP entity holds personal information about an individual, it must, on request by the individual, give access to the information.

APP 12.2 sets out a number of exceptions to the obligation in APP 12.1 for agencies.

APP 12.2 provides:

> *Exception to access - agency*
>
> *12.2 If:*
>
> *(a) the APP entity is an agency; and*
>
> *(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:*
>
> *(i) the Freedom of Information Act; or*
>
> *(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;*
>
> *then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.*

The Committee believes that the drafting of the preamble paragraph in APP 12.2(b) should be amended. The aim of APP 12.2 is to ensure that, if a request for access is made under the Privacy Act, an agency is permitted to refuse access under the Privacy Act if, had that request been made under the specified legislation that provides for access by persons to documents, the agency would have been required or authorised to refuse access under that legislation. In the Committee's view, APP 12.2(b) should be amended to read:

> *12.2 If:*
>
> *(a) a request for access under the Act is made to an agency; and*
>
> *(b) the agency would have been required or authorised to refuse to give the individual access to the personal information by or under:*

[3] See section 6 of the Privacy Act.

> *(i) the Freedom of Information Act; or*
>
> *(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;*
>
> *had the request for access been made under the legislation stated in subparagraph (i) or (ii),*
>
> *then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access by or under that other legislation.*

The Committee believes that APP 12.2 should be included in the form suggested above. There are certain grounds for refusal of access in the *Freedom of Information Act 1982* (Cth) that are not in the Privacy Act relating to the legitimate and special interests that the government may have in refusing access. The Committee submits that agencies should retain the right to refuse access on those other grounds.

The Committee further submits that APP 12.3 (exceptions to access for organisations on a wide range of grounds such as the request for access being frivolous or vexatious) should also apply to agencies, given the objective that the same principles apply insofar as possible to agencies and organisations. The grounds for refusal in APP 12.3 would seem to apply equally appropriately to agencies.

Section 16A and exceptions to APPs

The placement of some exceptions to the rules in the APPs in separate provisions may create confusion. For example, proposed Section 16A which specifies 'permitted general situations' in which collection, use and disclosure of certain information by certain entities is allowed despite the APPs. As the APPs will not on their own set out all the circumstances in which a use or disclosure may occur, non-lawyers may find it difficult to identify the relevant rules. The Committee suggests that notes be inserted in appropriate places in the Bill to draw the reader's attention to the existence and basic effect of those exceptions which are located in separate provisions rather than in the APPs.

Section 16B – permitted health situations and binding rules

Proposed section 16B allows the collection, use and disclosure of health information in certain situations despite the APPs. Proposed sections 16B(1)(b)(ii) and 16B(2)(d)(ii) allow collection of health information when it is done in accordance with "rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation".

The Australian Law Reform Commission (ALRC) made the following statement in paragraph 63.48 of its Report 108 about the equivalent phrase in NPP 10.2(b)(ii):

> *Both the [Office of the Privacy Commissioner] and the NHMRC stated that they were not aware of any existing 'rules established by competent health or medical bodies that deal with obligations of professional confidentiality' that would fulfil the requirements of NPP 10.2(b)(ii). No such rules were drawn to the attention of the ALRC in the course of this Inquiry, and no objections were raised in response to the ALRC's view, expressed in DP 72, to leave these provisions out of the 'Collection' principle. Consequently, the ALRC has not included this mechanism in the 'Collection' principle.*

Given this conclusion by the ALRC, and unless the Government is aware of the existence of any such rules, the Committee considers that the provisions containing the relevant words should be deleted. It appears that those provisions do not permit any collections, uses or disclosures that would not otherwise be permitted. The retention of those provisions might mislead providers of health services into thinking they have a lawful basis for collection, use or disclosure in the relevant circumstances, where this does not exist.

APP 7 – direct marketing

The Committee is concerned that the drafting of APP 7 in relation to the prohibition on the use or disclosure of personal information by organisations for direct marketing purposes may result in confusion. The Committee submits it may be unnecessary and misleading to have separate principles relating to personal information collected for the purposes of direct marketing and personal information collected for other purposes.

The Committee submits that APP 7 should be deleted, and appropriate direct marketing requirements be included in APP 6 relating to the use or disclosure of personal information generally, in the same way as they are included in the current NPP 2.1. The Committee has long supported appropriate measures to apply direct marketing restrictions consistently, regardless of the purpose of collection. This comment is directed merely to the implementation of that policy change, which the Committee submits could be achieved in a manner that would be understood by a non-expert within the generally applicable APP 6.

If this suggestion regarding APP 7 is not adopted, the Committee suggests that APP 7 be amended so that its logical structure follows that in APP 6 and in the corresponding NPP 2.

Currently, APP 7 relevantly provides:

> *7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.*
>
> *Exceptions—personal information other than sensitive information*
>
> *7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if …*
>
> *7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if …*

By contrast, APP 6 (in relation to use or disclosure of personal information) relevantly provides:

> *6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:*
>
> *(a) the individual has consented to the use or disclosure of the information; or*

(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if …

6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if …

The structure of APP 7 is a blanket prohibition on direct marketing, followed by a list of exceptions under which direct marketing is permitted. The structure of APP 6 is to prohibit use and disclosure of personal information unless certain circumstances apply. In the Committee's view, the structure of APP 7 suggests that direct marketing is generally prohibited unless an exception applies, whereas the structure of APP 6 is such that use and disclosure in certain situations is permitted and in all other cases it is prohibited. The Committee considers that the drafting reflects a different emphasis in approach regarding direct marketing on the one hand and use and disclosure of personal information on the other. The resulting structure in APP 6 is more permissive, whereas the structure in APP 7 is more prohibitive.

The Committee submits that direct marketing is a legitimate and economically valuable activity – much the same as use and disclosure of personal information for certain purposes other than the purpose for which it was collected - when conducted in a properly regulated way. The Committee believes that the approach to the subject matter would be better reflected if the drafting structure of APP 7 follows that used in APP 6.

APP 8 - cross-border disclosure of personal information

APP 8 sets out a requirement for an APP entity that chooses to disclose personal information to overseas recipients to take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs. Along with proposed Section 16C, APP 8 implements the new accountability approach to cross-border disclosure of personal information. This is reinforced in the note accompanying APP 8.1 which refers to proposed section 16C (which provides that in certain circumstances, an act done, or a practice engaged in, by an overseas recipient can be taken to be a breach of the APPs by the entity which disclosed the personal information to the overseas recipient).

APP 8 seeks to balance the public interest in the convenient flow of personal information outside of Australia and the public interest in compliance with the APPs outside of Australia. In an era of global trade and other interactions, the Committee believes that APP 8 errs too much on the side of cross-border compliance at the cost of the convenient flow of information.

For example, in striking this balance, the Committee submits that APP 8 may deter the growing use of cloud computing. The Committee submits that this may impede access for Australian businesses and other entities to the economic and other benefits that cloud computing has to offer, putting Australian businesses and other entities at a competitive disadvantage with their international counterparts.

The Committee submits that APP 8(1) should be redrafted to impose less onerous, but still effective requirements as follows:

(1) Before an entity discloses personal information about an individual to a person (the overseas recipient):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

the entity must take reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information in a manner which is inconsistent with the Australian Privacy Principles.

The Committee notes the exceptions within NPP 9.1(c) and (d) have not been included in the APPs, and submits that APP 8(2) should be amended to include the following exceptions:

the transfer is necessary for the performance of a contract between the individual and the organisation, 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 organisation and a third party.

The Committee reiterates its position that proposed section 16C should be redrafted to provide that, where an entity has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information in a manner which is inconsistent with the APPs, that entity should not be liable for any acts done, or practices engaged in, by the overseas recipient in relation to that information.

Part B - Credit reporting provisions

Style and structure of credit provisions

Further to the comments made above regarding drafting style and structure of the APP provisions, the Committee is concerned about certain structural elements of the Bill as it relates to the regulation of credit reporting.

One such concern is the structure whereby key concepts are defined in several places within the Bill,[4] but distant from the Part IIIA context in which they are used. The Committee is concerned that this drafting style may result in confusion of consumer rights by readers.

The Committee considers the use of multiple different named categories of credit-related information (such as credit reporting information, credit information, and credit eligibility information) may over-complicate the drafting. It is submitted that individual data elements may fall into one of these categories when originally collected, but may develop additional characteristics as they are used by a credit provider.

Effective reversal of onus of proof

The Committee is concerned about an effective reverse onus incorporated within multiple provisions in the Bill.

For example, Section 20C commences with subsection (1):

[4] For example in s 6 and proposed s 6G in Part II.

A credit reporting body must not collect credit information about an individual.

The subsequent subsections of Section 20C then provide a range of cumulative factual matters that permit the collection of credit information by a credit reporting body.

The Committee submits that it appears that in each case the credit reporting body will have a positive onus to demonstrate that each cumulative fact is in place at all times. The Committee considers that this may be an inappropriate requirement for credit reporting bodies that typically handle thousands or tens of thousands of files per day and are only able to do so effectively using significant automation.

The Committee submits that the effective reverse onus may hinder the development of competition in the market and cause credit reporting bodies to be excessively risk averse.

Arbitrarily large penalties

The Committee submits that a number of large penalties contained in the legislation are out of proportion to the gravity of the contraventions involved.

For example, the 2,000 penalty unit civil penalty for use or disclosure of credit reporting information if the information is false or misleading in a material particular in proposed section 20P is inappropriate in circumstances where a credit reporting body is reliant on other organisations for the accuracy or otherwise of much of the information that it holds.

The Committee regrets the availability of such significant penalties for events that may be trivial and may happen very quickly if an error arises. While the integrity of the current regulatory agencies is not open to doubt, the Committee feels it is important that legislation avoid making the capricious use of regulatory powers possible. This may be compared with the current section 18G, which provides that a credit reporting agency in possession or control of certain information must take “reasonable steps" to ensure that personal information is accurate, up to date, complete and not misleading.

Technical corrections

The Committee notes with regret that the legislation has been in its final form for a considerable period, despite including what the Committee considers to be shortcomings as indicated above.

The Committee understands, however, that the passage of legislation to make necessary improvements to credit reporting would be significantly delayed if these areas were re-examined or improved.

Accordingly, the Committee proposes to refer to several minor technical issues which it believes would be capable of being amended before the legislation is passed, and may improve the general useability of the legislation for credit reporting bodies, credit providers and consumers.

Pre-screening "opt out" - clause 20G

The Bill proposes to repeal the existing Part IIIA of the Privacy Act relating to credit reporting and substitute a new Part IIIA which will include proposed clause 20G. This clause generally prohibits the use or disclosure of credit reporting information for direct marketing purposes, then deals with pre-screening use and disclosures.[5]

[5] See Explanatory Memorandum, note 2 at p 138.

Pre-screening is a direct marketing process by which direct marketing credit offers to individuals are screened against limited categories of credit information about those individuals to remove individuals from the direct marketing credit offer, based on criteria established by the credit provider making the offer before the offers are sent.[6]

As noted in the Explanatory Memorandum, the pre-screening process generally involves the credit provider making the offer establishing the eligibility requirements for the offer and providing the list of individuals about whom the pre-screening assessment will be made. The credit reporting body undertakes the assessment and discloses it to a mailing house which conducts the direct marketing consistent with the assessment. The assessment is then destroyed.[7]

The Committee notes that the provisions as to pre-screening have been the subject of controversy, and that the Government has accepted that pre-screening as presently implemented may have economic value, while wishing to ensure an effective "opt out" mechanism.

The Committee's comment is directed at that opt-out mechanism. Subclauses 20G(5) to (6) permit an individual to request that a credit reporting body not use credit reporting information for the purposes of pre-screening. However, the consequence of that non-use is not spelled out. On one view, if such an individual were included in a file of potentially eligible individuals, and the credit reporting agency was not permitted to use credit reporting information in order to determine ineligibility, the individual would be required to "pass" the screening process, as no screening criteria could be used.

The Committee submits that this would be inappropriate, and may lead to an increased rate of credit invitations being offered to persons who may not have the capacity to service that credit.

A more practical measure may be for a credit reporting agency (or perhaps all credit reporting agencies) to establish a separate database of pre-screening opt-out individuals. All customer lists for which pre-screening had been requested would initially be "washed" against this opt-out list and the opted-out persons removed from the prospects list, before any use was made of credit information referred to in clause 20G(2). It should be expressed in proposed section 20G that an opted out person would not receive the credit offer proposed to be offered to persons who are successfully screened.

The Committee submits that it would be preferable to include express statements that no written record must be made of an opted-out individual being removed from a marketing list, and that no communication of a consumer's opted out status should be made to the credit provider or their agent under section 20G.

Destroyed or de-identified information - clause 23A

The Committee is concerned by the drafting in clause 23A which allows a consumer to make a complaint about acts or practices of credit reporting bodies or credit providers which may amount to breaches of certain provisions of Part IIIA or the registered Credit Reporting Code, particularly as the complaint may relate to personal information that has been destroyed or to de-identified information.

Once information has been effectively de-identified it will have (by definition) no connection to the complainant. In the Committee's view, particularly having regard to the very limited ways in which de-identified credit related information may be used under

[6] Ibid.
[7] Ibid at pp 138-139.

clause 20M, it would be inappropriate for a consumer to believe that wholly de-identified data based on their history was included in a data set of de-identified information.

The Committee submits that clause 23A(4) should be clarified so that it is clear that a complaint about information that has been destroyed or de-identified may relate to use of the information before that destruction or de-identification, or the fact of that destruction and de-identification, but not events following the destruction or de-identification.

In the usual course, the credit reporting body or credit provider may have limited ability to respond to a complaint about data after it has in fact been destroyed or effectively de-identified, which raises some doubt about the appropriateness of such complaints being able to be brought in the Federal Court.

"Australian link" requirement

The Committee is concerned about some of the credit reporting provisions requiring an Australian link, including the “Australian link" requirement where a foreign service provider is subject to Australian Prudential Regulation Authority (APRA) approved standards. For example, a credit provider is not permitted to provide credit eligibility information to an entity that has no Australian link (clause 21G(3)(c)(ii)).

The Committee understands that some authorised deposit taking institutions have established outsourcing operations with entities based in foreign countries as a means of providing financial services more economically and contributing to lower overall prices. These services may comprise "cloud" based technologies for data storage and backup, which may utilise storage in a variety of locations for the purposes of effective disaster recovery. In other cases, business processes (that may include automated credit decisioning or first line call centre support) may be hosted offshore by contracted service providers.

The offshore entities may be wholly-owned but foreign incorporated subsidiaries, or may be unrelated bodies subject to strict service agreements which require information to be used and dealt with solely for the purposes of the principal with high levels of security.

The Committee submits that the "Australian link" distinction is inherently artificial. If an Australian body has a 100% held subsidiary performing outsourced services in a foreign country, the control that it exercises would not change depending on whether the subsidiary is incorporated in Australia, in the relevant foreign jurisdiction, or another foreign jurisdiction.

The Committee submits that, at least where the credit provider is an authorised deposit-taking institution under the Banking Act 1959 (Cth) and the use of an offshore provider is consistent with standards set by APRA under ‘Prudential Standard CPS 231 Outsourcing’[8] and is subject to APRA's supervision, then the requirement for an Australian link should not apply.

Conclusion

The Committee welcomes the updating of the privacy regime and sees this as a good opportunity to address some of the shortcomings in the current legal framework as well as to harmonise provisions. For the reasons outlined above, the Committee sees some

[8] See http://www.apra.gov.au/CrossIndustry/Documents/Prudential%20Standard%20CPS%20231%20Outsourcing.pdf.

scope for improvement and welcomes an opportunity to work with interested parties to maximise the opportunities presented by the law reform process.

Attachment A: Profile of the Law Council of Australia

The Law Council of Australia exists to represent the legal profession at the national level, to speak on behalf of its constituent bodies on national issues, and to promote the administration of justice, access to justice and general improvement of the law.

The Law Council advises governments, courts and federal agencies on ways in which the law and the justice system can be improved for the benefit of the community. The Law Council also represents the Australian legal profession overseas, and maintains close relationships with legal professional bodies throughout the world.

The Law Council was established in 1933, and represents 16 Australian State and Territory law societies and bar associations and the Large Law Firm Group, which are known collectively as the Council's constituent bodies. The Law Council's constituent bodies are:

- Australian Capital Bar Association
- Australian Capital Territory Law Society
- Bar Association of Queensland Inc
- Law Institute of Victoria
- Law Society of New South Wales
- Law Society of South Australia
- Law Society of Tasmania
- Law Society Northern Territory
- Law Society of Western Australia
- New South Wales Bar Association
- Northern Territory Bar Association
- Queensland Law Society
- South Australian Bar Association
- Tasmanian Independent Bar
- The Large Law Firm Group (LLFG)
- The Victorian Bar Inc
- Western Australian Bar Association

Through this representation, the Law Council effectively acts on behalf of approximately 56,000 lawyers across Australia.

The Law Council is governed by a board of 17 Directors – one from each of the constituent bodies and six elected Executives. The Directors meet quarterly to set objectives, policy and priorities for the Law Council. Between the meetings of Directors, policies and governance responsibility for the Law Council is exercised by the elected Executive, led by the President who serves a 12 month term. The Council's six Executive are nominated and elected by the board of Directors. Members of the 2012 Executive are:

- Ms Catherine Gale, President
- Mr Joe Catanzariti, President-Elect
- Mr Michael Colbran QC, Treasurer
- Mr Duncan McConnel, Executive Member
- Ms Leanne Topfer, Executive Member
- Mr Stuart Westgarth, Executive Member

The Secretariat serves the Law Council nationally and is based in Canberra.