Submission to the House Standing Committee on Social Policy and Legal Affairs on the Privacy Amendment (Enhancing Privacy Protection) Bill 2012

August 2012

1. Background

The Australian Law Reform Commission's Report 108, *For Your Information: Australian Privacy Law and Practice* (**ALRC Report 108**), was released in August 2008. The Commonwealth Government issued its First Stage Response to the ALRC's Report 108 in October 2009, which considered 197 of the ALRC's 295 recommendations. The Commonwealth Government has indicated that its Second Stage Response will follow once the First Stage Response has been implemented.

The former NSW Attorney General referred the issue of privacy to the New South Wales Law Reform Commission (**NSW LRC**) in 2006, and requested that the NSW LRC liaise with the ALRC. Since then, the NSW LRC has issued five reports. The NSW LRC's overarching recommendation is that NSW should adopt the Unified Privacy Principles (**UPPs**) recommended by the ALRC, to achieve national uniformity.

On 24 June 2010 the Commonwealth Government released exposure drafts of legislation containing the proposed Australian Privacy Principles (**APPs**) and credit reporting provisions. These exposure drafts were referred to the Senate Standing Committee on Finance and Public Administration for report and inquiry (**Exposure Draft Inquiry**).

The Senate Finance and Public Administration Committee released its report on the draft APPs, entitled '*Exposure Drafts of Australian Privacy Amendment Legislation: Part 1 – Australian Privacy Principles*' (**Exposure Draft Report (APPs)**) in June 2011. The Committee released its report on the credit reporting provisions in October 2011, entitled *Exposure Drafts of Australian Privacy Amendment Legislation: Part 2 – Credit Reporting'*. The Commonwealth Government responses to these reports were tabled in May 2012.

The *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth) (**Bill**) has now been referred to the House of Representatives Standing Committee on Social and Legal and Policy Affairs and the Senate Standing Committee on Legal and Constitutional Affairs for inquiry and report.

The NSW Department of Attorney General and Justice[1] (**NSW DAGJ**) made a submission to the Exposure Draft Inquiry, relating primarily to the proposed APPs. Some aspects of that submission are reiterated in this submission.

This submission does not comment on the extent to which the draft Principles should apply to NSW at any future date nor does it set out the final position of the NSW Government on these issues.

2. National Consistency

In the First Stage Response to the ALRC's Report 108, the Commonwealth Government accepted two of the ALRC's recommendations regarding national consistency in privacy regulation.[2] It also stated that there are clear benefits to nationally consistent privacy regulation in the private sector, including the health sector, and that that it will work with State and Territory counterparts to progress privacy reforms.[3]

However, the proposed APPs will not apply to State and Territory Government agencies. Also, the Bill does not exclude the operation of state and territory legislation that concurrently regulates the handling of personal information by the private sector. For example, the *Health Records and Information Privacy Act 2002* (NSW) regulates the handling of 'health information' by both the public and private sectors in NSW. Therefore, the problems that the ALRC identified regarding inconsistency, lack of clarity, and fragmentation between Commonwealth and State and Territory privacy legislation remain.

It may be that the Commonwealth Government intends to pursue the adoption of the APPs by States and Territories once the Bill is passed. However, at that stage it may be difficult for the APPs to be amended to take account of States and Territory concerns. Furthermore, even if States and Territories considered the terms of the APPs acceptable, the APPs are generally not drafted in a way which would allow adoption by States and Territories without amendment.

NSW DAGJ accepts that obtaining the agreement of all jurisdictions to uniform privacy principles is a challenging task, particularly in light of the fact that some jurisdictions do not have equivalent privacy legislation applying to their public sector bodies. Nevertheless, there is clear benefit in a nationally consistent scheme.

3. Simplicity and clarity

The ALRC report recommended that the privacy principles in the Privacy Act should generally be expressed as high-level principles, and should be simple, clear and easy to understand[4]. The Exposure Draft Report (APPs) recommended that the draft APPs be redrafted with a view to improving clarity[5]. Unfortunately, as a whole, the

[1] Formerly the NSW Department of Justice and Attorney General.
[2] ALRC Report 108 Recommendations 3-1 and 3-2.
[3] First Stage Response at 21.
[4] ALRC Report 108, Recommendation 18-1.
[5] Exposure Draft Report (APPs), Recommendation 1.

APPs are significantly more complex, lengthy, and difficult to understand than the UPPs proposed by the ALRC.

4. Health Information

The ALRC made several recommendations relating to the treatment of 'health information' in the *Privacy Act 1988* (Cth) in chapter 63 of Report 108. The Commonwealth Government's First Stage Response to the ALRC's Report 108 accepted the majority of these recommendations.

The Companion Guide issued with the Exposure Draft in 2011 noted that there would be further public consultation on specific privacy protection principles relating to health. It does not appear that such consultation has taken place yet. Instead, it appears that the 'status quo' with regard to the treatment of 'health information' has been maintained in the Bill. NSW DAGJ understands that the Commonwealth Government intends to further consult on the handling of health information, rather than incorporate this into the Bill[6]. This may be a concern, given that once the Bill is enacted it will apply to health information from the outset.

There are several issues with regard to the regulation of 'health information' in the APPs, including:

- The ALRC recommended an exemption to the collection principle where an entity providing a health service collects information from a third party about family medical history[7]. The Commonwealth Government's First Stage Response accepted this recommendation, indicating that this would be incorporated into the *Privacy Act 1988* (Cth), and that this would avoid the need for the Privacy Commissioner to make further Public Interest Directions (**PIDs**) on this matter[8]. However, this is not reflected in the 'permitted health situations' described in section 16B.

- APPs 3.4(c) and 6.2(d) provide for exemptions for organisations to the collection, use and disclosure principles where a "permitted health situation" exists[9] "Permitted health situations" are defined in the proposed section 16B. However, it is not clear why these exemptions are only available to private organisations and not public agencies.

- Section 16B(2) provides for a "permitted health situation" exemption where collection is necessary for the "*management, funding or monitoring of a health service*". However, the "permitted health situation" disclosure and use exemptions in section 16B(3) do not contain an equivalent exemption.

---

[6] The website of the Commonwealth Attorney General states that "*[t]he remaining parts of the Government's first stage response (relating mainly to health services and research provisions) and the ALRC recommendations that it is yet to respond to will be considered in due course after the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 has been progressed*" (http://www.ag.gov.au/Privacy/Pages/Privacy-Reforms.aspx)

[7] ALRC Report 108, Recommendation 63-1

[8] First Stage Response at 133

[9] APPs 3.4(c) and 6.2(d)

Therefore, NSW DAGJ submits that the Commonwealth Government should commence consultation on the regulation of 'health information' by the APPs in light of the recommendations in ALRC Report 108 as a matter of priority.

5. The Australian Privacy Principles

APP1 - Open and transparent management of personal information

- NSW DAGJ's submission to the Exposure Draft Inquiry noted that the requirement that an entity take reasonable steps to make its privacy policy electronically available, as proposed by the ALRC,[10] was not included in APP1. The Exposure Draft Report (APPs) noted that the Department of Prime Minister and Cabinet did not support this proposal, on the basis that an absolute requirement to provide an electronic copy would be a significant burden on organisations without a website or means to otherwise produce an electronic copy[11]. Therefore, the Exposure Draft Report (APPs) recommended that a note be added at the end of APP1.5 indicating that the appropriate form of an entity's privacy policy will usually be online,[12] which was accepted in principle in the Commonwealth Government's response.[13]

  However, the note inserted at the end of AAP1.5 only provides guidance on where entities *will* usually provide their privacy policy, rather than how entities *should* make that policy available.

  Accordingly, it is submitted that the note at APP1.5 should be reworded to clarify that the 'appropriate form' for a privacy policy would usually be online on the entity's website. In the alternative, it is submitted that the Privacy Commissioner should issue guidelines to this effect.

- NSW DAGJ's submission to the Exposure Draft Inquiry noted that it may be preferable for privacy policies to contain not only "the purposes for which the entity … discloses personal information" but also some description of the individuals or entities who are most likely to receive it. This is crucial in terms of giving members of the public a real picture of how personal information is handled and to answer the question: "who are they giving it to?".

  The ALRC did not think this necessary if entities were required to set out a general description of disclosure practices.[14] APP1.4 arguably does not require this as it states only that the *purposes* of disclosure be described. This is a different question to the identity of persons or entities to whom disclosures will likely be made. As presently drafted, an entity might interpret APP1.4 in a manner that led to no description of the latter.

  The ALRC also considered that the obligation under the notification principle (now in APP5.1(f)) to provide information about usual disclosures made it

[10] ALRC Report 108, Recommendation 24-2.
[11] Exposure Draft Report (APPs), at 51-52
[12] Exposure Draft Report (APPs), Recommendation 6
[13] Government Response to Exposure Draft Report (APPs), at 6
[14] ALRC Report 108 at 820.

unnecessary to require this in a privacy policy.[15] However, notifying individuals in this manner is different to including such matters in a privacy policy which benefits the public at large. Individuals may wish to peruse a privacy policy before entering into any interaction with an entity and before the requirement under the notification principle applies. A requirement to describe the persons to whom disclosures are usually made would complement, not duplicate, the inclusion of this matter in the notification principle.[16] A requirement of this sort is unlikely to impose any significant burden on entities.

APP2 – Anonymity and pseudonymity

- NSW DAGJ's submission to the Exposure Draft Inquiry noted that, as presently phrased, APP2 could be read to require *either* the option of anonymity *or* pseudonymity. The ALRC recommended that both options should be available. The drafting of the principle could make this clear, for example, by replacing the term "or" with the term "and". There could be an exception from the requirement to provide both these options if one is not practicable, perhaps through an amendment to APP2.2. For example, pseudonymity may be practicable where anonymity is not, and in this case an entity should only be required to make the former available

  The Exposure Draft Report (APPs) noted that the Committee was "*concerned that a number of submitters were of the view that APP 2 does not provide a clear option of both anonymous and pseudonymous interactions.*"[17] However, the redraft of APP2 in the Bill does not address this concern.

- The ALRC's view was that the qualifications to the principle relating to lawfulness and practicability would be sufficient to address most agencies' concerns about the operation of this principle. As suggested by the ALRC, agencies should be able to gain further guidance about this principle from guidelines issued by the Office of the Australian Information Commissioner.[18]

  Guidelines on the circumstances in which compliance is to be considered impracticable under APP2 should set out matters to be considered in deciding whether compliance is practicable. They could make clear, for example, as suggested by the ALRC, that anonymity or pseudonymity generally will not be lawful in the provision of government benefits.

APP3 - Collection of solicited personal information.

- The protection provided by APP3.1 appears to be significantly weaker than that provided for in UPP2. APP3.1 provides that "*If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the agency's activities*" (emphasis added). Similar wording appears in

[15] ALRC Report 108 at 821.
[16] See ALRC Report 108 at [24.51] – [24.52] in relation to other matters to be included in privacy policies.
[17] Exposure Draft Report (APPs) at 61.
[18] ALRC Report 108 at 65.

relation to the collection of sensitive information in APP3.3. Notably, APP3.2 provides for stronger privacy protection for information collected by private organisations, as it omits the words "or directly related to". The Explanatory Note to the Bill acknowledges that the 'directly related' test "*may, depending on the circumstances, be a slightly lower threshold*"[19].

Under APP3.1 the only nexus required for collection is that the information is directly related to an activity of the agency, not that the collection would be necessary for (or even assist) that activity. If it is not necessary for an entity to collect information in order to perform its activities it is questionable why it should be entitled to do so.

As noted by the ALRC, the High Court has noted that the "*[t]here is, in Australia, a long history of judicial and legislative use of the term 'necessary', not meaning essential or indispensable, but as meaning reasonably appropriate and adapted*".[20]

The equivalent IPP in the *Privacy and Personal Information Protection Act 1998* (NSW) provides that:
"*(1) A public sector agency must not collect personal information unless:*
(a) the information is collected for a lawful purpose that is directly related to a function or activity of the agency, and
(b) the collection of the information is reasonably necessary for that purpose."[21]
(emphasis added)

Similarly, the equivalent IPP in the *Information Privacy Act 2000* (Vic) provides that "*[a]n organisation must not collect personal information unless the information is necessary for one or more of its functions or activities*."[22]
(emphasis added)

No compelling justification has been put forward as to why Commonwealth agencies require a lower threshold than those of equivalent State agencies in NSW and Victoria. The APPs should represent best practice privacy legislation. Therefore, it is submitted that the words "or directly related to" should be omitted from APP3.1 and APP3.3.

- NSW DAGJ's submission to the Exposure Draft Inquiry noted that it would be preferable to allow entities to collect information from third parties where an individual gives their express consent. NSW DAGJ is pleased to note that APP3.6 has now been amended to allow collection by agencies in such circumstances.

  However, the same facility has not been extended to private entities. The rationale for this distinction is not clear. The NSW Law Reform Commission recommended that an entity should be able to collect personal information about an individual from a third party if the individual consents, as is currently the case

[19] Privacy Amendment (Enhancing Privacy Protection) Bill 2012, Explanatory Memorandum, at 75.
[20] *Mulholland v Australian Electoral Commission* (2004) CLR 181 at 39.
[21] *Privacy and Personal Information Protection Act 1998* (NSW), section 8(1).
[22] *Information Privacy Act 2000* (Vic), schedule 1, IPP1.1.

under s9 of the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIPA**).[23] The NSW LRC's proposed "consent" exception, as the Commission pointed out, gives individuals autonomy about how their personal information may be collected.[24] An individual may prefer to have an entity gather their personal information from third parties rather than having to keep interacting with the entity. This may be an important matter of convenience for individuals as well as entities.

- APP3.3 permits the collection of sensitive information with the consent of the individual concerned. Section 6 of the *Privacy Act 1988* (Cth) defines consent to include express or implied consent.

  However, there are difficulties arising from the concept of consent. Ideally such consent should be voluntary, informed and express. However, the application of the concept is far from simple. For example, consent may be affected by social disadvantage such as illiteracy or a lack of knowledge about the right to refuse to give information. There is also the question of "bundled consent", that is, where an entity bundles multiple requests for an individuals' consent to a wide range of uses and disclosures of personal information, without giving the individuals the option of selecting to which uses and disclosures he or she agrees.

  Given these difficulties, it may be appropriate to limit consent in APP3.6 and APP3.3 to "express consent". The problem of "bundled consent" could be partially addressed by guidelines issued by the Privacy Commissioner.

- The terms of UPP2.2 and NPP1.2 include a requirement that information must not be collected in an "*unreasonably intrusive way*". Similarly, IPP 3(d) provides that collection must not "*intrude to an unreasonable extent upon the personal affairs of the individual concerned*". This requirement acknowledges that the way in which entities collect information has privacy implications, in addition to the content of that information.

  This prohibition is absent in APP3.5, which only provides that an APP entity must collect information by "*lawful and fair means*". Whilst the Explanatory Memorandum states that the word "fair" extends to an obligation not to use means that are unreasonably intrusive[25], this requirement should be made explicit in the terms of the legislation to provide clarity for APP entities.

  Accordingly, it is recommended that APP3.5 be amended to provide that information must not be collected in an unreasonably intrusive way.

APP4 – Receiving unsolicited personal information

- NSW DAGJ's submission to the Exposure Draft Inquiry noted that APP4, as drafted, required that all unsolicited information be assessed to determine if the information *could* have been collected under APP3, and if the answer is yes, then APPs 5-13 must be complied with. The ALRC's Recommendation 21-3, if

[23] NSW LRC Report 123 at [2.46].
[24] NSW LRC Report 123 at [2.46].
[25] Privacy Amendment (Enhancing Privacy Protection) Bill 2012, Explanatory Memorandum, at 77.

implemented, would have allowed an agency, if it did not wish to retain unsolicited information, to destroy it without having to decide whether it could have collected the information under APP3. Recommendation 21-3 would also have allowed the agency to destroy the information if it decided that it could have lawfully collected it, without the need to then comply with other privacy principles. It may be preferable to give agencies the option of destroying unsolicited information as the ALRC proposed.

The Exposure Draft Inquiry Committee considered that such a provision may address compliance burden concerns. However, the Committee noted that Commonwealth agencies, for example, must comply with the requirements of the *Archives Act 1983* (Cth) in relation to the destruction of records. Therefore, the Committee concluded that there may be merits for including such a provision but the interaction with other legislation would need to be considered.[26]

It is not clear whether consideration has been given to this proposal. The interaction between the *Archives Act 1983* (Cth) and APP4 could be clarified by explicitly providing within the *Archives Act 1983* (Cth) that destruction of unsolicited information under APP4 is an exemption to the general prohibition against disclosure in section 24 of the *Archives Act 1983* (Cth). Furthermore, even if it were not considered appropriate for Commonwealth agencies to be able to destroy such information due to requirements under the *Archives Act 1983* (Cth), this should not have any effect on this option being available to private organisations.

It is therefore submitted that this proposal be re-examined, as suggested in the Exposure Draft Report (APPs).

APP5 – Notification of the collection of personal information

No comment.

APP6 – Use or disclosure of personal information

- APP6.2(a) allows the use or disclosure of personal information for a secondary purpose if the "*affected individual would reasonably expect the entity to use or disclose the information for the secondary purpose*". NSW DAGJ submits that this should be amended to clarify that an agency must not use or disclose personal information for a secondary purpose in the face of an express objection from the individual.

- APP6.3 allows for an agency to disclose "biometric information" or "biometric templates" to an enforcement body, subject to guidelines issued by the Privacy Commissioner. This provision was not included in the Exposure Draft. The Explanatory Memorandum sheds little light on the justification for this inclusion, other than to assert that "*non-law enforcement agencies have current, and will have future, legitimate reasons to disclose biometric information and templates to law enforcement agencies*" and that "*there is a gap in the enforcement related*

[26] Exposure Draft Report (APPs) at 38.

activity exemption in the Privacy Act that prevents this increasing activity from occurring".[27]

There is no definition of "biometric information" or "biometric templates" in the Bill. The Macquarie Dictionary does not contain a corresponding definition of biometric information or biometric templates. The Biometrics Institute (Australia) describes biometric information as "*unique identifiable attributes of people used for identification and authentication. These include (but are not limited to) a person's fingerprint, iris print, hand, face, voice, gait or signature…*".[28] Biometric information could also include DNA material or profiles.

The Bill includes biometric templates and certain biometric information in the definition of "sensitive information".[29] This is line with ALRC' recommendation 6-4. The ALRC noted that:

> "*The definition of sensitive information should be amended to include certain biometric information. Biometric information shares many of the attributes of information currently defined as sensitive in the Privacy Act. It is very personal because it is information about an individual's physical self. Biometric information can reveal other sensitive information, such as health or genetic information and racial or ethnic origin. Biometric information can provide the basis for unjustified discrimination.*"[30]

The scope of APP6.3 is wide, as many government agencies may hold biometric information. As noted in ARLC Report 108,[31] in 2003, legislation was passed enabling officials to collect certain types of biometric information from non-citizens in Australia[32]. Also, in October 2005, the Commonwealth Government introduced the 'ePassport'—a passport with an embedded microchip containing, among other things, a digitised facial image of the passport holder.[33]

Under APP6.2(e), an agency may disclose information if it is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body. It is not clear why this exemption is not sufficient to disclose biometric information and templates to law enforcement agencies, where appropriate. APP6.3 contains no qualifier that the disclosure must be reasonably necessary for law enforcement activities conduced by an enforcement body – it merely needs to be made from an agency which is not an enforcement body to an enforcement body. The only qualification for the disclosure of such information is that it must be in accordance with guidelines issued by the Privacy Commissioner. However, such guidelines do not yet appear to exist, so it is not clear what the scope and limitations of this power will be. If any limitations are to be provided, they should be made in the *Privacy Act 1988*, as with other general exceptions to the APPs.

---

[27] Privacy Amendment (Enhancing Privacy Protection) Bill 2012, Explanatory Memorandum, at 80
[28] http://www.biometricsinstitute.org/pages/about-biometrics.html
[29] Privacy Amendment (Enhancing Privacy Protection) Bill 2012, section 42.
[30] ALRC Report 108 [6.119]
[31] ALRC Report [9.68]
[32] *Migration Act 1958 (*Cth) ss 5A, 40, 46, 166, 170, 172, 175, 188, 192.
[33] A Downer (Minister for Foreign Affairs), 'Australia Launches ePassports' (Press Release, 25 October 2005)

Biometric information can be a powerful investigative tool for enforcement bodies, and may be used as evidence in a prosecution. Therefore, the provision of biometric information from agencies to enforcement bodies where this is reasonably necessary for law enforcement purposes should be facilitated. Also, enforcement bodies may wish to share biometric information with other agencies for enforcement purposes, for example in the context of joint police operations.

However, it is submitted that before such APP6.3 can be supported, consideration must first be given to:

- Whether "biometric information" and "biometric templates" should be defined in the Privacy Act, such that it is appropriately limited but with scope to capture new forms of biometric technology as they become available
- What 'gap' there is in current law enforcement exemption which would prevent biometric information and templates being provided to law enforcement agencies under other law enforcement exemptions, where appropriate (e.g. APP6.2(e))
- What reasons agencies have to disclose such information to law enforcement agencies
- What use will be made of this information by law enforcement agencies
- The potential infringement of privacy and other risks that may be involved in such disclosure
- Whether the benefit to agencies in the disclosure of such information outweighs the infringement of privacy inherent in the disclosure
- What the scope and limitations for providing such information should be.

- As noted in NSW DAGJ's submission to the Exposure Draft Inquiry, the proposed "permitted general situation" at item 3 of section 16A[34] would allow an entity to use/disclose personal information if the entity reasonably believes the information is reasonably necessary to assist any entity, body or person to locate a missing person (and the entity complies with relevant privacy rules). The inclusion of a missing person exception is welcome. However, as it is currently drafted, this exemption may be too broad in some circumstances.

  This exemption would allow information, including sensitive health information, to be disclosed to any person or body to locate a missing person. This would include not just the Police, or other investigative agencies, but the missing person's family or a private investigator. It may not always be appropriate to allow personal information about a missing person to be disclosed to any person other than the Police (or other investigative agencies). A missing person might have gone missing for a number of reasons and may not want to be found by their family or other persons, for example persons leaving abusive relationships.

- No "research" exception to the use and disclosure principle has been included in APP6 (other than with respect to 'health information'), contrary to the ALRC's Recommendations 65-2, 65-4 and 65-9. The Commonwealth Government

[34] AAP6.2(g) in the exposure draft

accepted these recommendations in its First Stage Response to the ALRC's Report.[35]

It appears that the Commonwealth Government may intend to implement this aspect of ALRC Report 108 at a later stage, given that the Attorney-General's Department has stated that parts of the First Stage Response (relating mainly to health services and research provisions) will be considered after the Bill has been progressed[36]. However, once the Bill is enacted, without the benefit of the research exemptions, the collection, use and disclosure of personal information for research purposes may not be possible under the *Privacy Act 1988* (Cth).

It is therefore submitted that the Commonwealth Government should incorporate appropriate research exemptions into the Bill, in light of the ALRC's recommendations. Alternatively, temporary measures to facilitate such research should be implemented (e.g. by way public interest directions).

APP7 – Direct marketing

- APP7 leads to an anomalous outcome, in which an individual who consents to the use of their personal information for direct marketing receives *less* privacy protection if that information is sensitive information than if that information were non-sensitive information.

  Under APP7.2, where personal information (other than sensitive information) is collected from the individual and they would reasonably expect the information to be used for direct marketing, the organisation must provide them with a simple means by which they may easily request not to receive direct marketing communication from the organisation (or 'opt out'), and must cease to use the information if the individual opts out. Under APP7.3, where the individual would not reasonably expect the information to be used for direct marketing but consents to such use nonetheless, the organisation must also inform them of their ability to opt out of such communications in each direct marketing communication.

  However, under APP7.4 an organisation may use or disclose sensitive information about an individual for the purposes of direct marketing if the individual has consented to the use or disclosure of the information for that purpose. There is no requirement for the organisation to provide them with a simple means by which they can 'opt out', or for the organisation to inform them of their ability to opt out of such communications in each direct marketing communication.

  It is clearly anomalous for sensitive information to be provided with less privacy protection than non-sensitive information. By its very nature, sensitive personal information merits greater protection. Whilst an individual may have initially consented for the use of sensitive information for direct marketing, they may not

[35] First Stage Response at 53.
[36] http://www.ag.gov.au/Privacy/Pages/Privacy-Reforms.aspx

be aware that they can subsequently 'opt out' of receiving such information, or the means by which they can opt out.

This issue was raised before the Exposure Draft Inquiry Committee.[37] The Department of Prime Minister and Cabinet noted that under APP7.2 and AAP7.3 organisations would be required to provide a simple means by which an individual may easily request not to receive direct marketing communications from an organisation.[38] This would have been the case in the Exposure Draft. However, the redrafted APPs 7.2 and 7.3 explicitly exclude sensitive information, so this protection would not apply to sensitive information used for direct marketing. It is not clear whether this effect is intentional or a drafting error.

Accordingly, it is submitted that individuals who consent to the use of their sensitive information for direct marketing should receive no less privacy protection than if that information were non-sensitive personal information.

APP8 – Cross border disclosures of personal information

- APP8.1 provides that, before an entity discloses personal information to an overseas recipient, it must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs. However, APP8.2(a)(i) provides that APP8.1 does not apply if the entity "*reasonably believes the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information.*" Similarly, proposed section 16C, which holds an APP entity accountable for a breach of the APPs by an overseas recipient, does not apply if the entity satisfies AAP8.2(a)(i).

  The ALRC recommended that the Australian Government publish and maintain a list of overseas laws and binding schemes that effectively uphold principles for the fair handling of personal information that are substantially similar to the UPPs.[39] At the Exposure Draft Inquiry, the Department of Prime Minister and Cabinet noted that the Commonwealth Government would prepare a non-determinative list of countries with satisfactory privacy regimes for the purposes of APP8.2(a)(i).[40] However, there is no reference to this proposed list in APP8.2. Such a reference would be useful as it would both alert APP entities to the existence of this list, and could be used as an interpretive tool in determining whether an APP entity has complied with APP 8.2(a)(i).

  Therefore, it is submitted that APP8.2(a)(i) should explicitly refer to the non-determinative list of privacy compliant countries proposed to be prepared by the Commonwealth Government.

  Furthermore, it is submitted that the 'consent' exception in APP8.2(b)(ii) be limited to 'express consent'. As the effect of consent will be to remove an APP

[37] Exposure Draft Report (APPs) at 153
[38] Exposure Draft Report (APPs) at 153-154
[39] ALRC Report 108, Recommendation 31-6.
[40] Exposure Draft Report (APPs) at 179.

entity's obligations under AAP8.1 (and section 16C), it is appropriate that a higher threshold of consent be applied.

APP9 – Adoption, use or disclosure of government related identifiers

- As noted in NSW DAGJ's submission to the Exposure Draft Inquiry, the APP9 definition of "identifier" does not appear to include biometric information, as it is limited to numbers, letters, or symbols (or a combination of these objects).[41] This approach is contrary to the recommendations of the ALRC[42] and the NSWLRC[43] and should be further considered. The decision not to include biometric information in the definition of 'identifier' was apparently done on the basis that "*[t]he collection of such information by organisations will not result in the privacy risks that the 'identifiers' principle is intended to address, such as the risk of an identifier becoming widely held and applied to facilitate extensive data-matching or data-linking*."[44] However, it is possible that, especially with advances in technology, biometric data may be used in the same way as a set of numbers in that it may be passed to various entities and linked to certain information.

  The Exposure Draft Report (APPs) noted this submission, however referred to the Department of Prime Minister and Cabinet's response, which stated that "*to future-proof the types of identifiers regulated by the principle, the Minister responsible for the Privacy Act (rather than the Privacy Commissioner) will be able to determine what a government identifier is for the purposes of the Act*".[45]

  However, the definition of 'identifier' in the proposed section 6(1) of the *Privacy Act 1988* (clause 25 of the Bill) only provides a power for the Minister, by regulation, to *exclude* items from the definition of identifier. It does not provide the power for the Minister to *include* further items as identifiers, such as biometric information. Therefore, it is submitted that if biometric information is not to be included in the definition of identifier, the power for the Minister to prescribe further identifiers by regulation should be provided for in section 6(1).

APP10 – Quality of personal information

No comment.

APP11 – Security of personal information

No comment.

APP12 – Access to personal information

No comment.

[41] Proposed section 6(1) of the *Privacy Act 1988* (clause 25 of the Bill)
[42] ALRC Report 108, Recommendation 30-3.
[43] NSW LRC Report 123 at [10.32].
[44] First Stage Response at 74.
[45] Exposure Draft Report (APPs) at 202-203.

APP13 – Correction of personal information

No comment.

6. Definitions

- The Commonwealth Government should further consult with law enforcement agencies on the new definition of "enforcement related activity" in the Bill. The definition in the Bill appears to reflect more traditional and historical concepts of policing and may not adequately reflect the current important function and roles performed by modern law enforcement agencies.

  Also, as noted by the NSW LRC,[46] there is significant confusion around the phrase "for the protection of the public revenue" in subparagraph (e) of the definition of "enforcement related activity". The application of the concept to the collection of income in the form of fines or government charges for services is also unclear and should be clarified.

- The definition of "sensitive information" in section 6(1) of the *Privacy Act 1988* (Cth) currently includes "criminal history". The meaning of the term "criminal history" is not entirely clear but, as the NSW LRC pointed out, it may not extend to information about arrests and charges that do not result in a formal criminal record.[47] Such information is also very sensitive in nature and consideration should be given to including it in the definition.

- The Bill proposes to add the Immigration Department (currently the Department of Immigration and Citizenship (**DIAC**)) as an "enforcement body" in section 6(1) of the *Privacy Act 1988*. This provision was not included in the Exposure Draft APPs. This would have the effect of bringing DIAC within the enforcement related exemptions throughout the APPs.[48] Also, this would enable cross-border disclosure of personal information to overseas bodies that perform similar functions to those performed by DIAC.[49]

  The Explanatory Memorandum states that the rationale for this is that, *"[i]n view of DIAC's enforcement related functions and activities, and the type of information it collects, uses and discloses, it is appropriate to include it in the definition of 'enforcement body'."*[50] However, whilst DIAC may have some functions which could be considered to be similar to enforcement bodies (e.g. responding to breaches of immigration law), many of its functions are substantially different to other enforcement bodies (e.g. policy analysis, granting of visas, and assessment of refugee status). Therefore, if it may be more appropriate for DIAC to be subject to a more limited exemption, for example by way of a public interest direction issued by the Privacy Commissioner.

[46] NSW LRC Report 127, at [5.7(4)]
[47] NSW LRC Report 123 at [5.80].
[48] APP3.4(d), APP6.2(e), APP9.2(e) and 12.3(i)
[49] APP8.2(f)(ii)
[50] Privacy Amendment (Enhancing Privacy Protection) Bill 2012, Explanatory Memorandum, at 57.

- It is not clear from the definition of “court/tribunal order” in clause 12 (to be inserted at section 6(1) of the Privacy Act) whether the definition extends to courts and tribunals of the States and Territories.