SENATE STANDING COMMITTEE ON FINANCE AND PUBLIC ADMINISTRATION

LEGISLATION COMMITTEE

Exposure Drafts of Australian Privacy Amendment Legislation

SUBMISSION

SUBMISSION NUMBER: **25**

SUBMITTER

Professor Graham Greenleaf and Mr Nigel Waters

Cyberspace Law and Policy Centre
A Centre for the Public Interest in Networked Transactions

Necessary improvements to the Australian Privacy Principles

Submission to the Senate Finance and Public Administration Committee on the Exposure Draft of the Privacy Amendment Legislation

Graham Greenleaf and Nigel Waters[1], 13 August 2010

This submission to the Senate Finance and Public Administration Committee on its enquiry[2] into the Exposure Draft of the Privacy Amendment Legislation is from researchers at the Cyberspace Law & Policy Centre, UNSW Faculty of Law, and is the most recent in a series of detailed submissions we have made to the ALRC in 2006-08, and to the government since then, concerning proposed changes to the Privacy Act.[t6]

1 Overview

The proposed Australian Privacy Principles (APPs) are weaker than the ALRC's proposed UPPs and the current IPPs and NPPs, and unless significantly improved during the Parliamentary process will lead to an overall reduction in privacy protection. Regrettably, the government has gone backwards instead of forwards in terms of modernising the principles, and seems to have been unduly influenced by both business and agency interests, to the detriment of the interests of the citizens and consumers that the Privacy Act is intended to protect. In the case of government agencies, a raft of changes have been 'slipped in' at the last minute to avoid some agencies having to rigorously apply well-designed existing exceptions. Such lazy drafting and special pleading should be rejected.

There are a few improvements to the ALRC proposals in the government's draft Bill, but in many cases proposed changes to the language of the principles which appear minor and superficially innocuous in fact have very significant adverse effects. In particular, the cross-border disclosure principle, which has an ever-increasing importance in the context of borderless networks and 'cloud' computing, is seriously inadequate.

---

[1] Graham Greenleaf is a Professor of Law, University of New South Wales, and has been involved in privacy law and policy research and advocacy for 35 years. Nigel Waters is a former Deputy to the first Australian Privacy, a consultant on fair information practices, and principal researcher on the 'Interpreting Privacy Principles' project. The Cyberspace Law and Policy Centre has played a significant role in privacy law reform activity in recent years, with many submissions by us and our colleagues to the ALRC and to the subsequent government consideration of its Report. A list of submissions made through the Centre, and links to them, is at <http://www.cyberlawcentre.org/ipp/law_reform.htm>. The research underlying this and other submissions was done as part of an Australian Research Council Discovery Project 'Interpreting Privacy Principles'.

[2] <*http://www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/index.htm*>

Submissions: Improved APPs attached

Our submission are primarily contained in the attached 'Improved Exposure Draft'. Our proposed additions to and deletions from the Exposure Draft are visible from the change tracking to the document. Where we do not propose any changes to a section we have omitted the section. We have only proposed minimum changes to the wording of the APPs,where necessary to achieve better policy objectives. Small changes to this Exposure Draft can bring very considerable improvements to privacy protection. ***We recommend that the Committee adopt all of the changes to the Exposure Draft contained in our Improved Exposure Draft.***

Relationship of the APPs to other Privacy Act provisions

It is unfortunate that the government has released an Exposure draft of the APPs without drafts of other provisions relating to compliance and enforcement, and some coverage, exemption and definition matters not yet addressed. We understand the rationale for a staged release, and this is acceptable in relation to the specific credit reporting and health privacy rules. But a complete judgement as to the effect of changes to the principles can only be made in the context of the Information and Privacy Commissioners' functions and powers, and other parts of the Act, which may or may not change in the final amendment Bill.

2 Coverage of the Act

The Companion Guide to the Exposure Draft explains some of the government's intentions in respect of the coverage and application of the Act, once amended, including the effect of some changes in definitions.

We welcome the application of most of the APPs to 'entities' – both private sector 'organisations' and government 'agencies', although there are some exceptions which we submit are unnecessary. We comment on these in relation to specific APPs.

Definitions

The definitions relevant to the APPs, listed in Section 15 and Part 6 of the Companion Guide, are mostly uncontroversial. However there are a few significant ones.

The definition of '**enforcement body**' has been extended to include some additional agencies. Most of these additions are clearly of a similar nature to the existing ones, and are justified. But the addition of CrimTrac agency is of concern. Our understanding is that CrimTrac provides a range of common services, databases etc to operational law enforcement agencies – it has never in the past been considered an 'executive' agency with an independent law enforcement role. As such it is an inappropriate inclusion in this definition, and it is deleted in the Improved Exposure Draft.

A new definition - '**enforcement related activity**' - designed to capture the matters currently set out in NPP 2.1(h) has had a new element added to cover the conduct of surveillance, intelligence gathering and other monitoring activities. It is not clear why this is considered necessary, and has the potential to be very widely interpreted, and potentially misused to extend the effect of the exceptions which rely on the definition. The government needs to justify why any such activity necessary for law enforcement purposes is not already covered by the other parts of the definition. However, we have not deleted it in the Improved Exposure Draft.

The same definition also now includes 'other misconduct prescribed by the regulations ((e)). This would not need to be misconduct 'of a serious nature' which is the criterion for the main exception. When combined with the proposed new definition of '**misconduct**' to include 'any other misconduct in the course of duty' the net effect is to leave it open to future governments to significantly undermine the effect of some principles by Regulation. We submit that the parameters of the exceptions should remain specified in the Act. The addition of 'any other misconduct' would also weaken the effect of those principles to which the 'enforcement related activity' definition applies, even if no 'other conduct' was prescribed. We have deleted it in the Improved Exposure Draft.

The definition of '**personal information**' is re-worded from the ALRC recommendation but is not substantially different. We repeat our criticism of the definition from our response to the ALRC report:

> "This recommendation fails to ensure that the Act covers an increasingly important category of information which, while not in itself identifying an individual, allows interaction with persons on an individualised basis, or the imparting of consequences on an individualised basis. A broader definition is necessary partly to respond to technological change ... Replacing "reasonably identifiable" with "potentially identifiable" would go some way towards remedying this deficiency, but is not in itself adequate."

We have left this unchanged in the Improved Exposure Draft, as it requires comprehensive reconsideration in future.

The definition of '**solicits**' is essentially unchanged. We submit that it would be helpful to make it clear that it includes 'making a facility available for receipt of information' even if there is no express invitation or request. We have added this in the Improved Exposure Draft.

The meaning of '**consent**' is critical, but the government shows no signs of addressing one of the most significant weaknesses in the current regime, which was also avoided by the ALRC. We repeat our criticism from our response to the ALRC report:

> "The ALRC does not adequately address what is one of the most significant weaknesses in the current Act – the ability to interpret 'consent' in ways which completely undermine the effect of many of the principles. The definition of 'consent' should be amended to deal with a number of key issues concerning consent, specified in the following submission, rather than leaving them to [Privacy Commissioner] guidance. Other aspects of consent should be dealt with where possible in the Explanatory Memorandum, and only otherwise by ... guidance.
>
> Either the definition of 'consent' or the explanatory memorandum should state that consent, whether express or implied, must be clear and unambiguous, and should expressly state that a failure to opt out is not by itself to constitute unambiguous consent.
>
> The government should give further consideration to the implications of the confusion caused by the lack of any distinction in the Privacy Act between uses or disclosures justified by consent and those justified by acknowledgment of notification. At the least, the Act or the Explanatory Memorandum should state that where a person has no choice but to provide personal information in order to obtain a benefit, no consent to any uses of the information beyond the express purpose of collection may be implied. In such circumstances of 'involuntary consent', only express consent should apply.
>
> The definition of 'consent' needs to be amended in order to prevent abuse of the practice of 'bundled consent'. In particular, wherever consent is applicable to the operation of a privacy principle, separate consent should be required for each proposed purpose of use."

We have added these aspects in the Improved Exposure Draft.

Exemptions

We note that the government had previously indicated that it would not address the ALRC's recommendations concerning exemptions in the first tranche of amendments – putting them off until a second tranche of amendments at some unspecified future date. The Companion Guide restates this position in relation to the small business exemption, and is predictably silent on the political parties and media exemptions. It does however address the agencies and individuals exemptions.

We are disappointed that the government intends to make no changes to the exemptions for agencies, which the ALRC correctly criticised as being arbitrary. We urge the Committee to seek assurances from the government that these exemptions will at least be revisited in its second stage response to the ALRC report.

We support the restatement of the policy in s.16E of the existing Act, exempting acts or practices by individuals acting in a personal capacity. We submit that while privacy intrusive behaviour by individuals is a matter of concern, it is best addressed through a private right of action and other laws such as those dealing with surveillance.

We support the stated intention to continue the policy in s.7A of the existing Act which provides for certain acts and practices of 'agencies' to be treated as though they were 'organisations', although we submit that the current provision is too narrow, in that it applies only to agencies listed (arbitrarily) in a particular schedule in the FOI Act, and to prescribed agencies. We submit that to ensure that those APPs which apply only to organisations do apply also to commercial activities of government agencies, a broader 'deeming' provision is required. (See also our comments below on those APPs which do distinguish between agencies and organisations). We have not made any changes in the Improved Exposure Draft.

Emergencies and Disasters

We submit that the then government never provided a convincing justification for the insertion of Part VIA in 2006. We urge the committee to seek an explanation from the government as to why this Part is needed, with evidence of how (if) it has been used since 2006. We have not made any changes in the Improved Exposure Draft.

Extra-territorial operation

We support the proposed changes which will extend both the coverage of the Act and the Commissioner's ability to investigate acts and practices that occur outside Australia.

Acts or practices required by foreign law

We acknowledge that the policy in ss.6A4 and 13D of the existing Act needs to carry over, but draw attention to our major criticism of proposed APP8 (cross-border disclosure) which in our view does not require entities to be sufficiently careful in deciding into which foreign jurisdictions they can disclose personal information, which will expose personal information of Australians into many environments where foreign law, whilst binding, will fundamentally conflict with accepted Australian standards.

3 The Australian Privacy Principles (APPs)

Sequence and numbering

The sequence of the principles has been significantly changed from both the IPPs and the NPPs. The Companion Guide explains this as reflecting the 'life cycle' of handling personal information. While the change of Principle numbers will take some getting used to, it is, on balance, desirable – it would not have been possible to maintain direct equivalence.

Section 18 is intended "to ensure that the Principles can be referred to as Principles in the new Act". We assume this is to avoid the difficulty that has been caused by having all the NPPs in a Schedule. Making each Principle a separate section of the Act (but with numbering unlikely to coincide e.g. APP1 will not be section 1) risks the same confusion as has occurred with the NSW privacy legislation (the *Privacy and Personal Information Protection Act 1998 (NSW)*) with references to the principles and sections often being confused. For example, it is unclear whether it is intended that the provision in subsection (1) of APP1 would be formally referred to as APP1(1) or Privacy Act Section 2(1) (based on numbering in the Exposure draft which would of course change with incorporation into the Act).

However, balanced against this is that having each principle in a separate section means that the Act will work better in online research systems. This probably outweighs the above difficulties, so we do not propose any change.

APP 1: Openness

We support the requirement that entities (in both sectors) must have a 'clearly expressed and up-to-date privacy policy, covering specified matters. However, we submit that the list of matters needs to be made more consistent with the list of matters to be notified when collecting personal information, under APP5 (and both lists need to be expanded).

For example, under the current proposal, the privacy policy would have to specify 'purposes' (APP 1(4)(c) – as in APP5(2)(d)) but not usual recipients (APP5(2)(f) paraphrased). APP 1(4) requires information about how an individual may access information (d) and complain (e), but not 'identity and contact details' (APP5(2)(a)).[3]

APP1(4) requires the entity to include in its privacy policy information as to whether it 'is likely to disclose personal information to overseas recipients' (f) and if so, the countries in which such recipients are likely to be located' – but only 'if it is practicable to specify those countries' (g). (APP5(2)(i) & (j) specify the same information in relation to collection). Leaving aside the question of whether 'overseas' has the same meaning as 'outside Australia' in other provisions, the 'only if practicable' qualification is far too subjective, and is likely to lead to many entities not including this important information. In the context of APP8 (see below) both APP1 and APP5 are also deficient in not requiring any explanation of the level of privacy protection in the destination jurisdiction.

[3] see under APP5 for our submission that the latter requirement should specify 'functional' contact details

A further weakness of APP 1 is that the privacy policy need only be made available 'in such form as is appropriate' (5(b)) This is inferior to the ALRC's recommended UPP 4.2 which required that access must be provided 'electronically'. The requirement in APP1(6) for entities to respond to individual's request for the policy in 'a particular form' is only a partial and relatively weak substitute. It is also undesirable for APP1(6) to apply only to requests from *individuals* – it will often be *organisations* such as NGOs and the media which are seeking access to privacy policies, and this should be expressly accommodated.

Improvements based on the above submissions are in the Improved Exposure Draft.

APP 2: Anonymity and pseudonymity

We welcome the government's intention to expand the anonymity principle in the NPPs (NPP8) to include pseudonymity. But we fear that the provision as drafted inadvertently undermines the policy objective of encouraging anonymity as a preferred option, with pseudonymity as a 'next best' option. APP2 reads 'Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an entity.' Why would an entity offer the option of anonymity, if it can get away with offering pseudonymity (e.g. by provision of a non-identifying email address traceable via an ISP)? The Companion Guide suggests this is not what APP2 means. But it needs to be clarified that anonymity *must* be offered *where lawful and practicable* (as the NPP8 now provides), and that otherwise pseudonymity *must* be offered unless it is also unlawful or impracticable.

The principle has also been weakened, perhaps largely destroyed, by the re-wording of the exception. Instead of NPP8's positive formulation: 'wherever ... lawful and practicable', APP2 provides an exception, where an entity is 'required or authorised by or under law ... to deal with individuals who have identified themselves' ((2)(a), or where it is impracticable ((b)). Every government department must surely be so authorised by implication of one law or another? We submit that the policy objective is, or should be, to provide an exception where the identification *is required* by law etc (or impracticable).

Subject to fixing these two weaknesses, we support the explicit recognition of pseudonymity and the application of the principle to government agencies.

Improvements based on the above submissions are in the Improved Exposure Draft.

APP 3: Collecting solicited information

This principle is also significantly weaker than the equivalent NPP(1).

The existing limitation of collection to information 'necessary' for an entity's functions has been weakened to 'reasonably necessary' and the weaker formulation of IPP1 '*or* directly directly related to' has been added (APP3(1)). We submit that either 'necessary' alone or, preferably 'necessary *and* directly related to' would be an improvement.

APP3(1) could also be strengthened in other ways. We repeat our response to the ALRC recommendation:

> "The test needs to go to the reasonableness of the purpose rather than merely the reasonableness of information collection in the context of whatever functions or activity the organisation/agency specifies.

> The collection obligations should expressly link the amount of personal data that may be collected to the purpose of collection, and limit it to what is necessary for that purpose).
>
> The reference to 'purposes' could imply '*lawful* purposes', but we believe this should be made explicit as it is in IPP1, [and other privacy laws]. The principle should make it clear that collection can only be for a lawful purpose."

In relation to collection of sensitive information, we support the bringing forward of existing NPP 10.1 into APP3, although we submit that it is confusing to split the single list of 'conditions' in NPP 10.1 between APP3(2) and (3). (We note that existing NPP 10.2-10.4 deal with health information which the government will be addressing in separate exposure draft.)

However, the exceptions to 'consent' in 10.1 have been dramatically expanded in APP3(3). NPP10.1(b)'s 'required by law' has become 'required or authorised by or under ... in APP3(3)(a), without any justification for why the deliberately more protective wording has been abandoned in this specific context. We have previously accepted that 'specifically authorised' may be an appropriate change, but not the wholesale invocation of the very vague and subjective 'authorised'.

The 'emergencies' exception (NPP10.1(c)) has been broadened both by the removal of the 'imminent' threat criterion and by the addition of threats to an individual's 'safety' and to 'public health or safety' and by the replacement of the condition that consent be physically or legally impracticable with a much weaker 'unreasonable or impracticable to obtain consent' in APP3(3)(b).

The first two changes are generic and apply equally to the same exceptions to other principles. We repeat our response to the ALRC report:

> "There is currently no constraint on the ability of an agency or organisation to claim this exception for bulk or routinised uses or disclosures [and in this context, collections], as opposed to ad hoc, specific individual circumstances. The first part of the exception is by definition so limited – it will be necessary to identify specific individuals or small groups to satisfy this test. But if the exception was available for public health and public safety without the 'imminent' test, it is difficult to see how claims could not be made under it for a wide range of law enforcement and welfare programmes, including high volume data-matching and data linkage projects.
>
> We oppose the deletion of the qualifying word 'imminent' ... It is essential to retain a test of 'urgency; to justify why another basis for [collection] cannot be established (e.g. obtaining lawful authority, or by applying for a Public Interest Determination)."

The third change is a major weakening of the principle, and will be interpreted by entities to routinely justify collection of sensitive information without consent. The current wording of the condition in the NPP exception (NPP 10.1(c)(i)&(ii)) should be retained.

The 'investigation of unlawful activity' exception (APP3(3)(c)) was not included in the ALRC recommendation (UPP2.5). No explanation is offered as to why it is needed in the context of collection of sensitive information – while it may be, the government must justify it. If it remains, we submit that it should be conditional on the entity taking some 'appropriate action' within a reasonable period of time. Without such a condition, the exception invites the compilation and indefinite maintenance of 'blacklists' based on suspicion of wrongdoing, but without any requirement for individuals on such lists to be afforded natural justice.

The enforcement exception (APP3(3)(d)) is necessary, but is in our view undesirably broadened (and the principle consequently weakened) by the changes to definitions already criticised above.

Completely new 'special pleading' exceptions have appeared in APP3 for the specific benefit of the diplomatic service (e) and Defence Forces (f), allowing them to avoid the principle the basis of their own 'reasonable belief'. We submit that this reflects a lazy approach to compliance – there is no reason why these agencies should not have to comply with APP3, taking advantage where appropriate of the other generic exceptions. Any case for additional exceptions should be argued rather than simply asserted.

A further new exception aimed at assisting in locating people reported missing (APP3(3)(g)) relies on an as-yet-unknown 'Australian Privacy Rule' (Regulation). We submit that if a case can be made for an additional exception it should be specified in the Principle itself. As the Companion Guide acknowledges, this issue is difficult from a privacy perspective as some missing persons choose not to be 'found', but this is all the more reason for the balance to be set out in the principle and not left to Regulations.

In relation to the proposed exception for non-government organisations (APP 3(3)(h)), we repeat our response to the relevant ALRC recommendation on which it is based:

> "We suggest a preferable alternative that refers directly to the definition of sensitive information in the Act, and adds the caveat that the activities must be lawful, to avoid the exception covering organisations [involved in] unlawful discrimination, race hate etc.

We also recommend the reinstatement of a further condition which has been left out without explanation. The exception should read:

(h) *all* of the following apply:
(i) the information is collected in the course of the *lawful* activities of a non-profit organisation *which requires the sensitive information for the fulfilment of its purposes*;
(ii) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities, *and*
(iii) *at or before the time of collecting the information, the organisation undertakes to the individual to whom the information relates that the organisation will not disclose the information without the individual's consent*."
(italics show differences from APP3(3)(h))

It is not clear why additional exceptions recommended by the ALRC, which we found uncontroversial, do not appear in APP3(3). These include:

> "… necessary for the establishment, exercise or defence of a legal or equitable claim";
> "… necessary for research and all of the following conditions are met …" and
> "… necessary for the purpose of a confidential alternative dispute resolution process" (although we submit that this exception should read '…alternative '*prescribed*' [ADR] process' to avoid self-serving adoption of schemes without credibility).

We also return to the 'preference' the collection of sensitive information to be with consent, as expressed now in APP3(2)(a)(ii) (and subject to all the exceptions in (3) already discussed above. We submit that consent in the context of sensitive information must be confined to 'express' consent, (the definition of 'consent' in the Act

includes 'implied' consent) – see also our general comments above on the meaning of consent.

Improvements based on the above submissions are in the Improved Exposure Draft.

APP 4: Receiving unsolicited information

This requirement, suggested by the ALRC as UPPP 2.4, has been elevated into a separate principle, and APPs 5-13 specified as principles which are applicable to retained information. We support the substance of this provision.

APP 5: Notification of collection

We repeat the submission in our response to the ALRC Report that either the principle, or the definition of 'collects', should expressly include collection by observation, surveillance or internal generation in the course of transactions, to ensure that the notification principle is not read as applying only to collection resulting from 'requests'. This is particularly significant in relation to APP 5(2)(b), which applies where an entity collections personal information from *someone other* than the individual. This could be read as excluding the collection methods that do not involve a third party.

The required content of notification when information is collected is similar to that in NPP1.3 and the ALRC's proposed UPP3, but there are some significant differences.

As already mentioned above, we submit that APP5(2)(a) should specify '*functional* contact details' to prevent entities from allowing contact details to lapse or become ineffective – a depressingly common experience with 'customer complaints' addresses, telephone numbers and email addresses. A precedent exists in the Spam Act 2003, which requires a 'functional unsubscribe facility'.

We welcome the addition of a requirement to specify any relevant Australian law (or court or tribunal order) in APP5(2)(c). This will prevent entities relying on uninformative and unhelpful generalities, as many do under NPP1.3(e) and IPP 2(d).

It is not clear why the term 'body' has been introduced into APP5(2)(f) – the other two terms 'entity' and 'person' would seem to adequately cover the field.

The requirement to inform individuals about access, correction and complaint mechanisms has become expressly indirect – i.e. the requirement is only to direct people to the privacy policy (required under APP1) (APP5(3)(g) & (h)) – the ALRC's recommendation (UPP3 (c) & (g)) was ambiguous. While indirect notice of actual mechanisms is common practice due to understandable pressures to keep privacy notices concise, it is not clear why the simpler wording 'how the individual may...' is not adequate as this would implicitly allows a multi-step notice. It would be retrograde if many entities move to an indirect notice, and for those that do, more rigorous monitoring and enforcement of compliance with APP1 will be necessary, if individuals are to be guaranteed easy and effective access to their own information, and to remedies for breaches. We submit that these two exceptions should take the simpler form 'how the individual may ...'.

The addition of a specific requirement to include information about transfer to overseas recipients (APP3(3)(i) & (j)) is welcome, but suffers from the same weakness – the 'excuse' of impracticability) as does the equivalent provision in the requirement for a privacy policy in APP1. We repeat our concerns that the 'only if practicable' qualification is far too subjective, and is likely to lead to many entities not including this important information. In the context of APP8 (see below) both APP5 and APP1 are also deficient in not requiring any explanation of the level of privacy protection in the destination jurisdiction. We also again draw attention to the inconsistency in use of 'overseas' in APPs 1, 5 & 8, but 'outside Australia' in other provisions.

Improvements based on the above submissions are in the Improved Exposure Draft.

APP 6: Use and disclosure

The wording of APP7(1) should use (*a* **primary purpose**) and (*a* **secondary purpose**) rather than (*the* ...) to reflect the reality that an entity may have more than one primary or secondary purpose (this is already acknowledged by the use of the plural 'purposes' in other principles.

We note that this principle splits the single list of 'conditions' in UPP5 (and NPP2) between APP6(1) and (2) – it is not clear why this has been done and it is potentially confusing – (1) is not only meaningless without an understanding that (2) contains 'exceptions' to consent but is actively misleading in that it implies that consent has a much more prominent role than it does in reality. Having consent as just one of a number of conditions for use and disclosure in a single clause gives a much more realistic impression of the effect of the law.

In relation to the other conditions, we submit that the same range of criticisms we have outlined above in relation to the collection principle (APP3) apply equally to APP6. These relate to the following APP6 'exceptions':

(b) ... required or authorised by or under law ...

(c) ... threat to life health etc...

(d) ... unlawful activity or misconduct...

(e) ... enforcement related activities

(f) ... diplomatic etc functions ...

(g) ... missing persons

We refer to our comments and suggestions on these exceptions in relation to APP3.

We note that the ALRC's recommendation for an additional exception for alternative dispute resolution (ADR) processes has been included – as APP6(2)(i). As already noted in relation to APP3 (which omits this exception) we submit that the word 'prescribed' be added so that only bona fide ADR schemes would qualify.

An additional exception is proposed for uses or disclosures 'reasonably necessary for the establishment, exercise or defence of a legal or equitable claim' (APP6(2)(h)). This seems disproportionate as it requires no assessment of how trivial that claim may be in comparison with the effect on a person's privacy.

APP6(3) requires entities using or disclosing personal information under exception (e) – enforcement related activities – to make a written note. We submit that this important accountability requirement should extend at least to exceptions (d) (and (f) and (g) if they survive) which are of a similar kind to (e).

APP6(5) disapplies the general Use and Disclosure principle from any use or disclosure of personal information for the purpose of direct marketing, or of government identifiers. This is presumably intended to refer to use and disclosure that is subject to, respectively, APP 7 (direct marketing) and APP9 (government identifiers) although this link is not expressly stated – we submit that it should be, for clarity.

However, we also submit that this provision is unnecessary and harmful. It is a complete departure both from the ALRC's recommendations (UPPs 5, 6 & 10) and the existing NPPs 2 & 7, which have direct marketing and identifier principles as 'extra requirements' applying over and above the normal application of the use and disclosure principle (to the extent that they are compatible). We submit that the ALRCs recommendations for these activity and information specific principles, on which APP 7 and APP9 are based, were not designed as 'stand alone' regimes, and that the attempt to separate them would have unintended and undesirable consequences.

Improvements based on the above submissions are in the Improved Exposure Draft.

APP 7: Direct Marketing

Firstly, we submit that this principle should not apply only to private sector organisations, but should apply to all 'entitles'. We repeat our submission from our response to the ALRC Report:

> "We believe the principle should apply to both agencies and organisations on the grounds that the boundaries between private and public sectors are increasingly blurred, and government agencies are now commonly undertaking direct marketing activities. As we noted in our earlier submission, the equivalent principle in the Hong Kong Ordinance applies to all sectors, and the Hong Kong Privacy Commissioner has found public sector bodies in breach of it. Government agencies will still be able to justify some direct marketing campaigns – the proposed principle accommodates this, while giving individuals the choice not to receive some government communications through these channels. Governments can generally rely on generic 'broadcast' media to promote services, compliance issues etc."

We note the effect of section 7A of the existing Act which would apply APP 7 to commercial activities of some prescribed agencies, but we submit that this is not an adequate substitute for a generic application of the principle to all government agencies. We also note that the exemption for most agencies has been expressly extended to cover any contracted service providers (APP7(1)(c)), and consider this unnecessary, on the same basis. A generic change to 'entity' is in the Improved Exposure Draft.

With the application of APP 7 to agencies, there would also need to be an exception for where direct marketing communications were required or specifically authorised by law. This has been added to the Improved Exposure Draft.

The Companion Guide to APP7 makes a distinction between 'existing customers' and 'non-existing customers', on the basis of whether the individuals concerned have 'provided' personal information to the entity which is undertaking the direct marketing.

However, the expression 'collected the information from the individual' (not provided) is used in the Exposure Draft, and there is a risk that APP 7(2)(b) could be interpreted to include non-consensual collections. For the principle to achieve its objective, it is essential that the lesser protection afforded to 'existing customers' should only apply where the individual has knowingly and voluntarily provided the information. It would not be acceptable for individuals be denied an 'opt-out' either because their information had been collected without their knowledge (as is often the case in internet use) or because they had been required (e.g. by law) to provide it (as is the case with many financial, telecommunications and government transactions under statutory 'customer identification' requirements.

APP7 is poorly drafted in that it does not use the same distinctions as are explained in the Companion Guide. And furthermore the titles of the subsections (2) and (3) do not accurately reflect the content. Both of these clauses (2) and (3) are 'conditions', differentiating direct marketing on the basis not only of whether information is collected from an individual or from a third party, but also on the basis of 'reasonable expectation'. Clause (3) applies both to third party collection and to collection from an individual who 'would not reasonably expect ...' while (2) applies to collection from individuals who 'would reasonably expect...' . No guidance is provided as to how 'reasonable expectation is to be assessed, and in any case the practical effect of the distinction is not clear. Under (2) the organisation has to have provided a simple means (to opt-out') while under (3) the organisation must also have taken steps to notify the 'opt-out' (d) and must have consent (unless impracticable) (b). The relationship between reasonable expectation; consent; provision of notice, and the existence of a means to opt-out is very unclear.

Also unclear is the operative relationship between the 'scope' clauses (2) and (3) and the other subsections – what is the meaning of 'this subsection' in these two clauses? A close reading reveals that (2) and (3) are in effect additional exceptions (as well as those in (1)(a) and (b)) to the prohibition on direct marketing in (1). But this would not be clear to most organisations subject to the principle. We submit that APP7 fails the fundamental test that legal obligations should be at least reasonably comprehensible.

The 'bottom line' of APP7 is that it does not in fact operate as a prohibition on direct marketing, other than where the information used is sensitive information and the individual has not consented (APP7(1)(a)). It is otherwise merely a series of 'conditions' which apply to direct marketing activity, and would be better presented as such.

APP7(2) and (3) appear to have the effect of requiring all organisations to maintain a facility to allow people to 'opt-out' of direct marketing (which they would have to do under (5) in any case), but only those covered by (3) have to do anything to draw an individual's attention to it, and even then not with any prominence. Under (2), if the individual would reasonably expect to receive marketing communications, they are not even required to be notified – this seems perverse and is a very weak provision. All the evidence suggests that most individuals are only too aware that they are likely to receive direct marketing from organisations with which they have dealt, but that it is precisely these communications they wish to be able to stop!

Given that APP7(4) & (5) will give individuals the right to opt-out from any direct marketing communications from organisations, we do not understand why (2) & (3) are needed, since their only effect seems to be to limit the knowledge of that right.

A strong point of APP7 is that gives individuals an express right to request an organisation not to send direct marketing communications, and not to supply it to any other organisation (but not governments!) for that purpose (4)(a) & (b), and require organisations to honour such requests within a reasonable time and free of charge ((5)((a) & (b)). Individuals can also request an organisation to provide their 'source' ((4)(c)); i.e. to ask the question 'where did you get my name', but this is undermined by the broad exception where it is 'impractical or unreasonable' for the organisation to answer ((5)(c)) – we submit that this exception is highly likely to be abused.

We note that the major loophole of the exemption for charities is not addressed in this tranche of the draft legislation. We submit that individuals do not typically distinguish between commercial and charitable solicitations from a privacy perspective, and that they should have the same rights in relation to both.

The apparently strong condition for direct marketing involving 'sensitive information' in APP7(1)(a) – that it be with consent, is undermined by the general weakness that 'consent' is defined in the Act as including implied consent. We submit that in this context, express consent should be required – otherwise organisations will be free to use small print in terms and conditions, and 'bundled consent' to allow them to direct market using sensitive information.

Improvements based on the above submissions are in the Improved Exposure Draft.

APP 8: Cross-border disclosure

The most controversial new principle is APP8, which, at the urgings of the ALRC, abandons what it calls a 'border protection' approach in favour of the approach mis-described as 'accountability' Given that the existing NPP9 in effect allows personal data to be exported to any country (not matter how weak its laws) if 'reasonable steps' are taken to ensure that the data is used consistently with the NPPs, and that Australian law has not developed any interpretation of what are 'reasonable steps', the differences in the Australian context are probably more apparent that real. The real issue is whether what is proposed is any better than the current extremely weak protection.

Under APP8(1), an Australian company or agency will be able to send personal information anywhere in the world (subject to APP6). If it is not completely exempt from any liability for what then happens to the information (under nine separate exemptions), then it will be liable under the Australian Act for any acts by the overseas recipient that would breach the APPs if the APPs applied to it (s20). This applies to acts by any overseas recipient, even one that might be exempt under Australian law in Australia (for example, a 'small business'). The Australian exporter will also breach APP8 if it fails to take reasonable steps, before exporting data, to ensure that the overseas recipient does not breach the APPs (other than APP1). There is no definition of such steps, nor any proposed power for the Commissioner to issue guidelines or model contracts. We submit that it is essential that the Commissioner should issue guidelines concerning model clauses or a model contract clauses before any organisation can rely on a contract as meeting the 'reasonable steps' test in APP 8(1).

Curiously, the exporter does not have to take steps to ensure the importer complies with APP1, the only APP where it is relatively easy to prove that an overseas recipient is in breach (because it does not have an available Privacy Policy). And that indicates the main weakness: in relation to all the other APPs, how does an individual in Australia prove on the balance of probabilities how a breach has occurred in an overseas country, and one which by definition has no similar privacy laws of its own (if it did, the exporter would be exempt from any liability under one of the exemptions)? The purported 'accountability' remains a fiction. We submit that a breach by an overseas recipient should be a rebuttable presumption if damage to the individual can reasonably be assumed to have resulted from the export. That would be real 'accountability', but it is lacking at present. We have amended s20 to this effect, by addition of s20(3) to provide some reasonable prospect for complainants to enforce 'accountability' without facing insurmountable problems of onus and burden of proof..

Another weakness is that APP8 won't even require individuals to be given notice at the time that their data is going … somewhere or other. If organisations were required to give such notice, they would think twice before doing so, and individuals would be on guard for damage. We have already commented above on the weakness in APPs 1 & 5 that only require policies and collection notices to specify likely destination countries 'if practicable' and contain no requirement to explain the level (or lack of) privacy protection in those countries.

But APP8(1) is at least an attempt at regulation of overseas transfers. It is however fatally undermined by APP 8(2) which provides nine separate means by which a data exporter can be exempt from even the theoretical liability/'accountability' of APP8(1).

The first exception is where the exporter 'reasonably believes' in the existence of an overseas law or binding scheme, that 'has the effect of protecting the information in a way that, overall, is at least substantially similar' to the APPs, with mechanisms for redress and enforcement (APP(2)(a)). As we have emphasised in previous submissions, this is completely unacceptable basis for allowing cross border transfers. Some organisations will inevitably make self-serving judgements about the level of protection in other jurisdictions and/or pay for advice that supports their desire to transfer. Similar protection should be an exception to any prohibition on transfer, but it must be based on objective criteria. The only practical approach with the current Exposure Draft is simply to delete 'the entity reasonably believes that', so that the question of the effectiveness of the overseas privacy protections becomes a question of fact, to be determined initially by the Privacy Commissioner on the basis of a complaint, and ultimately by a court on appeal. Such ex post facto determinations may discourage exports of Australians' personal information to countries where privacy protection is questionable, but that would be a good result. It would be preferably if there could be some prior considered assessment of similarity or adequacy by experts, such as the Privacy Commissioner, and this could be achieved by guidelines under the current Act. A binding 'white list' scheme is a feature of privacy laws in some other jurisdictions and could usefully be adopted in Australian law, provided it was based on objective assessments, not politics. However, we have not included this in the Improved Exposure Draft, as it would be a major change and is not necessary.

The second exception is where there is consent based on explicit notice that the exporter accepts no liability ('accountability') for whatever happens overseas (2)(b). But there is no requirement for the organisation to explain the 'risk' either generally or in relation to the specific destination, and consent can still be 'implied' so this is likely to result in completely ineffective 'small print' notices tucked away in standard terms and conditions.

Another exception is where Australia is a party to some international agreement that relates to information sharing – this would in effect abrogate Australian sovereignty and is an example of 'policy laundering' – hiding behind often spurious claims of 'international obligations' to justify actions which would not otherwise be lawful.

Improvements based on the above submissions are in the Improved Exposure Draft. Although we reject the abandonment of a 'border control' approach that underlies APP 8, the existing NPP 9 is itself so weak that an improved APP 8 could be an improvement. It is not an improvement in its current form, but with the changes we propose, it would be an improvement on NPP 9. The two key changes are quite simple, and in our view, unarguable: (i) an objective standard for the level of privacy protection provided in another country; and (ii) more disclosure of the details of an overseas transfer to individuals before they are asked to consent to it (and thus lose their rights to any remedy).

APP 9: Government identifiers

The restrictions on the private sector using government identifiers have been strengthened by extension to the use of State or Territory government identifiers. However, APP9 only applies to the private sector (organisations), and the Use and Disclosure principle (APP6) now does not apply to an organisation (private sector) in relation to government related identifiers. Previously, both applied. In contrast, the government identifiers principle will not apply to the use of such identifiers by government agencies, but APP6 on use and disclosure will apply to such uses. The most significant abuse of government identifiers, data matching by government agencies, stays conveniently out of reach of APP9.

Improvements based on the above submissions are in the Improved Exposure Draft.

APP 10: Quality

Reasonable steps to ensure accuracy, currency and completeness of information collected is required, and relevance also required at the time of use or disclosure. These are conventional principles of international standard. We do not recommend any changes.

APP 11: Security and deletion

The security principle, and the requirement to delete or de-identify remain much the same and are also principles of international standard. We do not recommend any changes.

APP 12: Access

Access is not controversial in principle, but its technical details and exemptions can be. For government agencies, the principle defers to Freedom of Information legislation for

these matters. For organisations, the principle specifies the grounds for withholding and also sets out requirements for access processes, and allows for 'not excessive' charges, Compared to the ALRC's proposed access principle, additional grounds for withholding have been introduced, and others expanded, without any convincing justification. The Committee should look at this, but we do not recommend any changes.

APP 13: Correction

APP13 fixes a deficiency in the previous IPPs (federal government principles) by allowing individuals to request correction of records irrespective whether access to the records might be blocked because of an exemption from access. It also allows individuals to request that corrections be notified to any previous recipients of the corrected information from the entity concerned. This is an improvement, though it still leaves it the individual to identify the recipient, rather than to request 'please notify all previous recipients of the incorrect information'. it is likely that principle 12 would allow individuals to request a list of all previous recipients of information about them, so they could then lodge a list of requests for notificiaton. It would be a useful addition to APP 13 to include a Note to this effect, but we have not added that to the Improved Exposure Draft.