Australian Privacy Foundation

Privacy Amendment (Enhancing Privacy Protection) Bill 2012

Submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs

August 2012

email: mail@privacy.org.au

website : www.privacy.org.au

Please note that APF does not have a single postal address – we prefer communication by e-mail. If a postal address is required please contact the signatory.

Publication of submissions

We note that we have no objection to the publication of this submission in full. To further the public interest in transparency of public policy processes, APF strongly supports the position that all submissions to public inquiries and reviews should be publicly available, except to the extent that a submitter has reasonable grounds for confidentiality for all, or preferably only a limited part of, a submission.

Contents of this submission

1 Introduction – A Bill that should be rejected

The Australian Privacy Foundation (APF)

The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. Since 1987, the Foundation has led the defence of the right of individuals to control their personal information and to be free of excessive intrusions. For information about the Foundation see www.privacy.org.au

About this submission

This Bill has a complex structure and effect, with Schedules amending substantial parts of the existing Privacy Act 1988, and other legislation. While two Schedules deal with separate 'jurisdictions' within the Privacy Act – Information Privacy generally (in Schedule 1) and Credit Reporting (in Schedule 2) – some of the associated changes in relevant processes and definitions are contained in other Schedules, (primarily Schedule 4); Schedule 3 creates a new Part dealing with Codes, moving and revising provisions previously in two separate Parts, while Schedule 4 deals also with investigations, enforcement, powers and functions of the Commissioner

Dealing with the Schedules and clauses sequentially would obscure the significance of the important changes. We have therefore structured this submission around what we consider to be the main areas of change, bringing together comments on relevant clauses from the different Schedules. At the end of most explanation, we conclude with a specific submission about the relevant clause(s).

This submission refers to previous submissions from the Australian Privacy Foundation[1] and from researchers at the Cyberspace Law & Policy Centre, UNSW Faculty of Law[2], and is the most recent in a series of detailed submissions both bodies have made to the ALRC in 2006-08, and to the government and Parliament since then, concerning proposed changes to the Privacy Act. We draw the Committee's attention in particular to an **Improved Exposure Draft** of the Australian Privacy Principles (APPs) which was attached to Submission 25 to the Senate Standing Committee on Finance and Public Administration Legislation Committee[3].

Rejection or major overhaul of this Bill is needed

The government has 'cherry picked' the ALRC's recommendations and brought forward too many that are unfriendly to privacy, and ignored many of the ALRC's better recommendations. Ideally, this incomplete and consumer-hostile Bill should be defeated or withdrawn, and the government should bring back to the Parliament a Bill that comprehensively improves the *Privacy Act*. Failing that, and perhaps more realistically, this Bill should be given a thorough overhaul, adding those valuable ALRC recommendations now omitted, restoring those that have been weakened, and adding other vital improvements (such as the Commissioner's obligation to make decisions

[1] The APF's 100 page submission to the ALRC on Discussion Paper 72 is at <http://www.privacy.org.au/Papers/ALRC-DP72-0712.pdf >

[2] These can be found at <http://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=57970>

[3] Submission 25A, now also at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2025497>

where complainants are dissatisfied) that the ALRC unfortunately missed. One way or another, this Bill needs to be salvaged from its present unsatisfactory state.

The government claims there is another privacy reform Bill, the one containing all the hard bits, just over the horizon, but within the lifespan of the current government. After a four year wait for the first Bill, it is hard to take that claim seriously. This is the Parliament's 'once in lifetime' chance to adopt meaningful and overdue privacy reforms, and it should make sure all necessary reforms are included in this Bill.

Submission 1: The Parliament should ensure that all necessary and desirable privacy reforms are included in this Bill, as the opportunity is unlikely to come again.

Little help to Australia's international position

Australia has still not received an 'adequacy' finding for its privacy law from the European Union, whereas in 2011 the key EU 'Article 29' committee gave the green light to an adequacy finding for New Zealand. Accession to Council of Europe data protection Convention 108 by non-European countries is also now being actively promoted, and it may evolve to become a global convention which guarantees free flow of personal information between its members. This Bill does little overall to advance Australia's case for adequacy or accession, because of its data export changes, its incomplete appeals provisions, and its continuance of exceptions which have received international criticism. Whether the stronger enforcement powers can compensate is questionable. Internationally, this seems like a missed opportunity for Australia.

Submission 2: The Parliament should consider the benefits that can be obtained for Australia's international trading position, and international reputation, by stronger reforms than are found in this Bill.

2 Stronger Commissioner's powers: No use if not used

While we support the Commissioner having stronger powers, we consider that successive Commissioners have had a history of inaction in the use of the enforcement powers that they do have, which has seriously undermined the effectiveness of the Privacy Act. It has made complainants feel that they are powerless, and has sent a signal to businesses and agencies that compliance with the Privacy Act is in reality 'optional' for many purposes, and that breaches of the Act do not pose a significant business risk. This regrettable situation cannot be reversed solely by more powers or more resources being given to the Commissioner. More powers must also be given to complainants so that they can ensure for themselves that the Commissioner does his or her job. There also needs to be a change of approach by the Office of the Australian Information Commissioner in relation to its Privacy Act functions, to emphasise pro-active enforcement and public demonstration of this, rather than the historical focus on behind the scenes settlement of non-compliance cases.

Appeals are useless if no decisions are made

There is a hidden reform in this Bill: for the first time, there is a right of appeal to the Administrative Appeals Tribunal (s96(1)(c)) against decisions by the Commissioner to make a 'determination' of a complaint under s52(1) or (1A) (the only type of enforceable decisions about complaints under the Act). This long-overdue reform is one that privacy advocates and others have been demanding for over a decade. But it is not mentioned in the Second Reading Speech, nor in the Explanatory Memorandum. Perhaps it is too embarrassing to mention it, because for the right of appeal to have any meaning, the Commissioner would first have to made decisions against which appeals can be lodged. The current Commissioner has made one s52 determination during his time in office, and the previous Commissioner did not make one single determination in her whole five years in office. In the 23 year history of the Privacy Act, successive Commissioners have made a mere nine determinations[4]. It is a very poor record of inaction.

Therefore, this new right of appeal is of little use unless complainants can require the Commissioner to make formal decisions under s52 of the Act. Successive Commissioners, including the current one, have adopted a policy that complainants have no right to a formal decision even though they disagree with the Commissioner's view that a complaint has been successfully resolved. As a result, many dissatisfied complainants are denied even a formal determination dismissing their complaint under s52(1)(a) – and without such a formal decision, they will have no right of appeal. The Commissioner has confirmed that he is sticking to this 'you have no right to a decision' policy in Fact Sheets 10-12, issued in June 2012. The only way to make the new s96 right of appeal meaningful is therefore for the Commissioner to be required to make a formal decision dismissing a complaint, whenever a complainant so requests, so as to activate a complainant's right of appeal. Unless this is done, the new right of appeal will be useless, a theoretical right negated by the Commissioner's inactivity in this important function. It is a ridiculous situation, but it is how the Act currently works.

[4] The database of determinations is at < http://www.austlii.edu.au/au/cases/cth/PrivCmrACD/> and there is one subsequent determination since incorporation into the Information Commissioner's office.

Previous government proposals to allow such dissatisfied complainants to go direct to the Federal Court have been dropped, but were not good enough in any event: the Commissioner should be required to make a decision where the complainant reasonably requests one, so that normal appeal rights are available to them. Furthermore, the cost of proceedings in the Federal Court usually exceeds $100,000, so this is not a remedy which is of any use to most complainants.

Complainants are most likely to want a formal resolution of their complaint when they are dissatisfied with the Commissioner's proposed settlement in mediation of a complaint, or where the Commissioner considers (but the complainant disagrees) that the respondent has taken reasonable steps to resolve the complaint. However, the right to a formal decision should be available wherever the Commissioner proposes to refuse or cease investigation of a complaint, on whatever ground.

Submission 3: The Privacy Commissioner should be required to make a determination under s52 wherever a complainant so requests, and for complainants to be informed that they are entitled to such a formal resolution of their complaint. If this is not provided, the new s96 right of appeal against determinations will be meaningless, because (on 23 years past experience) the Commissioner will not make determinations to appeal against.

Other aspects of the Commissioner's discretion to arbitrarily dispose of complaints also need to be reigned in: he/she can refuse to investigate complaints wherever he/she thinks investigation 'is not warranted', an unwarranted and un-appealable discretion; and he/she can recognise another dispute resolution scheme to substitute for the Privacy Act, even if it provides lesser remedies than the Act, depriving complainants of their rights. The powers of the Privacy Commissioner can, paradoxically, sometimes be a hazard to privacy protection.

Submission 4: The proposed power of the Commissioner to refuse to investigate a complaint wherever he/she thinks investigation 'is not warranted' (new s41(1)(da)) is an unwarranted and un-appealable discretion, and should be deleted.

Submission 5: The Commissioner's powers to recognise another dispute resolution scheme (s35A), and to refuse to investigate a complaint on the grounds that it is being or could be dealt with under such a scheme (new s41(1)(dc) and (dd)), should be limited to apply only to such schemes as provide at least the same remedies as are available under s52 of the Privacy Act.

Enforcement strengthened, but still major gaps

This Bill makes other improvements to the Commissioner's powers that are significant, but they are incomplete (compared with the ALRC's recommendations), and in some cases defective. Their effectiveness also presupposes a more active Commissioner than has been the case.

Submission 6: The Privacy Foundation supports the other largely positive reforms to the Commissioner's powers (including the proposed changes to s52(1)(ia)), s52(1A)), s13G, s33D, s33E and s35A), subject to suggesting the following improvements.

Broadening of the complaint determination power, to allow the Commissioner to direct respondents to take specific actions to remedy a complaint (s52(1)(ia)), is very desirable.

New civil penalty provisions in s13G for 'serious' or 'repeated' breaches, for which the Commissioner will have to apply to a Court, are desirable. However, the criteria for these breaches to occur are not clearly defined.

The new power to make determinations following 'own motion' investigations (s52(1A)), is highly desirable. In the hands of a sufficiently motivated Commissioner, it could be the strongest and most effective enforcement mechanism in the Act.

Allowing for the Commissioner to accept enforceable undertakings (s33E) is highly desirable, particularly as this does not require a prior finding of an 'interference with privacy'. Similar procedures have worked well in the South Korean data protection legislation for over a decade. It is particularly desirable that 'the Commissioner may publish the undertaking on the Commissioner's website' (s33E(5)), but we consider that this should be strengthened to require the Commissioner to make such undertakings public, but with an option for an undertaking to be anonymised where the privacy interests of an individual make this necessary.

Submission 7: The Commissioner should be required to make enforceable undertakings obtained under s33E public, but with an option for an undertaking to be anonymised where the privacy interests of an individual make this necessary.

New powers to require Privacy Impact Assessments (PIAs) from agencies (s33D)) are desirable. However, they are defective in not requiring PIAs to be either independent or public. Many PIAs have apparently been conducted in Australia, but few have been made public to assist in public debate on important initiatives. Most importantly, there is no provision to ensure that requested PIAs are completed before decisions are made to proceed with the activity in question.

Submission 8: The Commissioner should make public a direction to an agency under s33D(1) to conduct Privacy Impact Assessment (PIA). The Commissioner, upon receiving a PIA, should be required to make it public.

Submission 9: An agency should be prohibited from carrying out, or making a final decision to carry out, the proposed activity or function which are the subject of a PIA, until the Commissioner has made the PIA public.

Assessments function

A new function to conduct 'assessments' of the compliance of any public or private sector organisation in relation to its compliance with the APPs or other forms of enforceable privacy principles (s33C) replaces the audit function of the Commissioner - currently applying only to Commonwealth agencies and to tax file number and credit information - with a new 'assessment' function applicable to all APP entities – but this is curiously located outside the 'monitoring' functions, and without the benefit of the important 'powers' clauses that currently apply. TFN and credit information remains subject to the separate 'monitor' and 'examine records' functions, which do have those associated powers. It is not clear if the overall effect is to effectively extend full audit powers to all private sector organisations with obligations under the Act, as recommended by the ALRC (Rec 47-6).

Submission 10: The Commissioner's new 'assessment' function should be clarified to ensure that it does effectively extend full audit powers to all APP entities.

Mandatory data breach notification should be included in this Bill

The ALRC's proposed requirement on businesses to notify consumers and the Commissioner of any major breaches of data security is not included. Mandatory data breach notification provisions are already part of the privacy laws of South Korea and Taiwan, and are either already in place or being enacted in many other jurisdictions around the world (particularly in many jurisdictions in the USA), so why not here after six years of law reform? This is the one likely opportunity for such reform. Such a scheme needs careful design, with appropriate thresholds and perhaps a two stage process, but there are many precedents, and operational experience available.

Submission 11: A mandatory requirement to notify significant data breaches both to the data subjects affected, and to the Commissioner, should be included in this Bill.

3 Australian Privacy Principles (APPs): Comprehensively weaker

Overview of the APPs

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 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.

Relationship of the APPs to other Privacy Act provisions

It is unfortunate that the government released an Exposure draft of the APPs (in mid 2010) 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 was acceptable in relation to the specific credit reporting rules (released as an Exposure draft in early 2011), and might also have been appropriate in relation to health privacy rules, promised as part of the first stage reforms but which have not now been delivered. But a complete judgement as to the effect of changes to the main principles could only be made in the context of the Information and Privacy Commissioners' functions and powers, and other parts of the Act. These had been expected to be the subject of another Exposure draft Bill but have only recently been made public in the final amendment Bill now before the Parliament, with wholly inadequate time for full consideration and debate.

Definitions – Inadequate

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 (Schedule 1, Item 16) 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.

Submission 12: CrimTrac should be deleted from the list of enforcement bodies.

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 (Schedule Item 20 – definition – (b)). 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.

The same definition also now includes 'other conduct prescribed by the regulations' ((f)). This would not need to be misconduct 'of a serious nature' which is the primary criterion in (f). 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 conduct' would also weaken the effect of those principles to which the 'enforcement related activity' definition applies, even if no 'other conduct' was prescribed.

Submission 13: The phrase 'other conduct prescribed by the regulations' should be deleted from the definition of 'enforcement related activity'.

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 consider this 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.

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."

South Korea's amended data protection legislation of 2011 is a model for the types of amendments that are required.

Submission 14: The definition of 'consent' in s6(1) needs to be amended in order to prevent abuse of the practice of 'bundled consent'; to state that consent, whether express or implied, must be clear and unambiguous; and to expressly state that a failure to opt out is not by itself to constitute unambiguous consent.

Unjustified exemptions need to be removed by this Bill

While general exemptions from the Act are not addressed in the Bill, and are relevant to more than just the APPs, we address the issue in this part of our submission as their main effect would continue to be to deny individuals the privacy protection of the principles (the APPs in the future) in some major areas of Australian life.

The government has 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.

It is therefore no surprise that removal of unjustifiable exemptions from the Act ('small' business; employee records; and political matters), as proposed by the ALRC, is omitted from this Bill. Australians deserve better than to wait forever for a second reform Bill – there should be one comprehensive Bill including all reforms.

Submission 15: The Bill should be amended to include removal of the exemptions for 'small' business operators (s6C(1)); employee records (s7B(3)); and political acts and practices (s7C).

The Bill includes no changes to the exemptions for agencies (s7), which the ALRC correctly criticised as being arbitrary. Where agencies can make a case for exemption from specific principles or other obligations, this needs to be argued on a case by case basis.

Submission 16: The ALRC's recommendations on removing exemptions for agencies should be included in this Bill.

Some powerful government agencies, such as Defence and Foreign Affairs, have even negotiated arbitrary and unjustified exceptions from some Principles. Under proposed s16A (s16A(1) Table Item 3 and s16A(2)), further exemptions from some of the APPs can also be created by the Privacy Commissioner, but unlike the existing Public Interest Determination procedures, without any public hearings, notice or opportunity for public scrutiny. No such exemptions should be created by the Commissioner unless there are previous public hearings equivalent to the Public Interest Determination procedures, followed by the usual disallowance procedure for a legislative instrument.

Submission 17: The Commissioner's powers to make exemptions from the APPs under new s16A without any public hearings should be amended to require that there be public hearings equivalent to the current Public Interest Determination procedures.

We support the restatement of the policy in s16E and s7B(1) of the existing Act, exempting acts or practices by individuals acting in a personal capacity.

Submission 18: 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 s7A 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).

Submission 19: 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 in s7A.

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.

Submission 20: Part VIA of the Act should be deleted unless the government can provide a convincing explanation for its retention.

The Bill has taken a new approach to provision of exceptions to some of the Principles. Instead of listing all of the applicable exceptions within each Principle, some of the common exceptions (applicable variously to the collection, use and disclosure principles) have been taken into a separate new section outside the APPs – s16A – Permitted general situations. While this may save a few words in some Principles, it is extremely unhelpful to the clarity of the law – it will be much less obvious, from a simple reading of an APP, what its scope and effect will be. If one set out to design the law so as to deliberately obscure a layperson from understanding its effect, the introduction of s16A would be an ideal tool.

Submission 21: Section 16A should be deleted and the relevant exceptions spelt out in each APP to which they apply.

APP 1: Openness – No disclosure of overseas recipients and their laws

APP 1.4 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). (APP 5.2(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.

The list of matters requiring disclosure in an organisation's privacy policy needs to be made more consistent with the list of matters to be notified when collecting personal information, under APP 5 (and both lists need to be expanded). The privacy policy would have to specify 'purposes' (APP 1.4(c) – as in APP 5.2(d)) but not usual recipients (APP 5.2(f) paraphrased).

Submission 22: In the context of APP 8, disclosure of the countries in which recipients will be (or might be) located should always be required. If an organisation does not know (or is not willing to say) where personal information is going, it should not send it there.

Submission 23: In the context of APP 8, both APP 1 and APP 5 are also deficient in not requiring any explanation of the level of privacy protection in the destination jurisdiction.

Submission 24: The privacy policy should also always disclose the usual recipients of personal information, whether located in Australia or located overseas.

APP 2: Anonymity and pseudonymity

The expansion of the anonymity principle in the NPPs (NPP 8) to include pseudonymity is desirable in theory. However, APP 2 as drafted (either inadvertently or intentionally) undermines the policy objective of encouraging anonymity as a preferred option, with pseudonymity as a 'next best' option. APP 2 reads 'Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP 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 current version of APP 2 effectively destroys the anonymity principle in NPP 8.

Submission 25: APP 2 must be clarified to state that anonymity must be offered where lawful and practicable (as NPP 8 now provides), and that otherwise pseudonymity must be offered unless it is also unlawful or impracticable.

The application of the principle to government agencies is also desirable, but APP 2 has also been weakened, perhaps largely destroyed, by the re-wording of the exception. Instead of NPP 8's positive formulation: 'wherever ... lawful and practicable', APP 2 provides an exception, where an entity is 'required or authorised by or under law ... to deal with individuals who have identified themselves' (2.2(a)), or where it is impracticable (2.2(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 only where the identification is expressly *required* by law etc (or impracticable).

Submission 26: The previous positive formula should be reinstated, so that APP 2 applies 'wherever lawful and practicable'.

APP 3: Collecting solicited information – Existing limitations abandoned

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 IPP 1 '*or* directly related to' has been retained for the benefit of agencies, but not private sector organisations (APP 3.1).

Submission 27: APP 3 should provide collection of information should be limited to either where 'necessary for' (alone) or, preferably both 'necessary for and directly related to' the primary purpose.

For 'sensitive information', the exceptions to 'consent' in NPP 10.1 have been dramatically expanded in APP 3.3 and 3.4. NPP 10.1(b)'s 'required by law' has become 'required or authorised by or under ... in APP 3.4(a), without any justification for why the deliberately more protective wording has been abandoned in this specific context. We reject the wholesale invocation of the very vague and subjective 'authorised'.

The 'emergencies' exception (NPP 10.1(c)) has been broadened in s16A ('permitted general situations') firstly by the removal of the 'imminent' threat criterion, secondly by the addition of threats to an individual's 'safety' and to 'public health or safety' (all in Item 1(b) of the Table in s16A(1)) and thirdly by the replacement of the condition that consent be physically or legally impracticable with a much weaker 'unreasonable or impracticable to obtain consent' in Item 1(a) of the Table.

The first change is generic and applies equally to the same exceptions to other principles (not just to 'sensitive information'. 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)."

Submission 28: The qualifying word 'imminent' should be reinstated in all 'emergencies' exceptions (wherever they are located). It is essential to retain a test of 'urgency'; to justify why another basis for collection cannot be established.

The second and third changes in APP 3 in relation to 'sensitive information' are major weakening of the principle, and will be interpreted by entities to routinely justify collection of sensitive information without consent.

Submission 29: The current wording of the condition in the NPP exception (NPP 10.1(c)) (paraphrased as where there is a ... threat to life or health of any individual) should be retained in relation to sensitive information.

Submission 30: The current wording of the condition in the NPP exception (NPP 10.1(c)(i)&(ii)) (paraphrased as where consent is physically or legally impracticable) should be retained in relation to sensitive information.

The 'investigation of unlawful activity' exception (Item 2 in the Table in s16A(1) and invoked by APP 3.4(b)) was not included in the ALRC recommendation (UPP 2.5). 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.

Submission 31: The exception in APP 3(4)(c) should be deleted or coupled with a requirement of enforcement action being taken within a specified and reasonable time.

Completely new 'special pleading' exceptions have appeared in APP 3 for the specific benefit of the diplomatic service (Item 6 in the Table in s16A(1)), the Defence Forces (Item 7 in the Table) – both invoked by 3.4(c) , allowing them to avoid the principle the basis of their own 'reasonable belief', and for the Immigration Department (by the addition of APP 3.4(d)(i) for the benefit of this Department alone). 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.

Submission 32: The special exemptions for the diplomatic service, Defence Forces and Immigration Department should be deleted, as they have not been justified.

A further new exception aimed at assisting in locating people reported missing (Item 3 in the Table in s16A(1) and invoked by APP 3.4(c)) relies on an as-yet-unknown Commissioner's legislative instrument. We submit that if a case can be made for an additional exception it should be specified in the Principle itself. As the previous Companion Guide to the Exposure Draft acknowledged, 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.

Submission 33: The exception aimed at assisting in locating people reported missing should be stated in the Act, not in an as-yet-unknown Commissioner's legislative instrument.

Submission 34: The proposed exception for non-profit organisations (APP 3.4(e)) should refer directly to the definition of sensitive information in the Act, and add the caveat that the activities must be lawful, to avoid the exception covering organisations [involved in] unlawful discrimination, race hate etc.

APP 4: Receiving unsolicited information

This requirement, suggested by the ALRC as UPP 2.4, has been elevated into a separate principle, and APPs 5-13 specified as principles which are applicable to retained information.

Submission 35: We support the substance of APP 4.

APP 5: Notification of collection – remaining deficiencies

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 NPP 1.3 and the ALRC's proposed UPP 3, but there are some significant differences.

Submission 36: APP 5.2(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'.

The addition of a specific requirement to include information about transfer to overseas recipients (APP 5.2(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 APP 1. In the context of APP 8 (see below) both APP5 and APP 1 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.

Submission 37: APP 5.2(j) is deficient in that the 'only if practicable' qualification is far too subjective, and is likely to lead to many entities not including this important information, and in not requiring any explanation of the level of privacy protection in the destination jurisdiction.

APP 6: Use and disclosure – The principle is misleading

The wording of APP 7.1 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 the previous UPP 5 (and currently in NPP 2) between APP 6.1-6.3. It is not clear why this has been done and it is potentially confusing and misleading. Sub-section (1) is not only meaningless without an understanding that 6.2 and 6.3 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.

Submission 38: APP 6 needs to be rewritten so as not to be confusing and misleading, Consent should be only one of a number of conditions for use and disclosure, with all exceptions in a single clause, so as to give 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 (APP 3) apply equally to APP 6. These relate to the following APP 6 'exceptions', :

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

(c) – invoking the following 'general permitted situations' exceptions from Table 1 in s16(1):

- threat to life health etc...
- unlawful activity or misconduct...

- diplomatic etc functions ...
- missing persons ...

(e) ... enforcement related activities

Submission 39: We make the same criticisms and suggestions in relation to the exceptions to APP 6 as we made above in relation to APP 3.

We note that the ALRC's recommendation for an additional exception for alternative dispute resolution (ADR) processes has been included – as item 5 in Table 1 in s16A(1), invoked in relation to use and disclosure by APP 6.2(c).

Submission 40: 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' (Item 4 in Table 1 in s16A(1), invoked by APP 6.2(c)).

Submission 41: The exception in relation to legal or equitable claim is disproportionate as it requires no assessment of how trivial that claim may be in comparison with the effect on a person's privacy.

APP 6.7 requires entities using or disclosing personal information under exception (e) – enforcement related activities – to make a written note. Logically, this safeguard should apply to all exceptions which are of an 'exceptional' nature i.e. likely to be used only occasionally.

Submission 42: The important accountability requirement in APP 6.7 should extend other exceptions of a similar 'exceptional' kind to (e).

APP 6.7 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 APP 9 (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 ALRC's recommendations for these activity and information specific principles, on which APP 7 and APP 9 are based, were not designed as 'stand alone' regimes, and that the attempt to separate them would have unintended and undesirable consequences.

Submission 43: APP 6 should apply to the activities covered by APP 7 (direct marketing) and APP 9 (government identifiers).

APP 7: Direct Marketing – Complex, confusing and weak

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."

Submission 44: APP 7 should not apply only to private sector organisations, but should apply to government agencies as well, i.e. to all 'APP entities'.

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 (APP 7.5), and consider this unnecessary, on the same basis. 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.

APP 7.2 and 7.3 and 7.6 appear to have the effect of requiring all organisations to *maintain a facility* to allow people to 'opt-out' of direct marketing, but only those covered by 7.3 have to do anything *to draw an individual's attention to it*, and even then not with any prescribed level of prominence. Under 7.2, 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 APP 7.6 and 7.7 appear to give individuals the right to opt-out from any direct marketing communications from organisations, we do not understand why 7.2 and 7.3 are needed, since their only effect seems to be to limit the knowledge of that right.

APP 7.6 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 government agencies!) for that purpose, and to require organisations to honour such requests within a reasonable time and free of charge. Individuals can also request an organisation to provide their 'source'; i.e. to ask the question 'where did you get my name', although this is undermined by a broad exception in 7.7 where it is 'impractical or unreasonable' for the organisation to answer – we submit that this exception is highly likely to be abused.

Submission 45: The Direct Marketing Principle should be simplified and strengthened, including by requiring notification of opt-out and related rights in every marketing communication.

We note that the major loophole of the exemption for charities and political solicitations (also embedded in the Spam and Do Not Call Register regimes) is not addressed in this Bill. 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 APP 7.4 – that it be with consent, is undermined by the general weakness that 'consent' is defined in the Act as including implied consent.

Submission 46: In the context of APP 7.4, 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.

APP 8: Cross-border disclosure – Fictional accountability, no real protection

The most controversial new principle is APP 8, 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 NPP 9 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 APP 8.1, an Australian company or agency will be able to send personal information anywhere in the world (subject to APP 6). 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 APP 8 if it fails to take reasonable steps, before exporting data, to ensure that the overseas recipient does not breach the APPs (other than APP 1). 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 APP 1, 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 APP 8 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 APP 8.1 is at least an attempt at regulation of overseas transfers. It is however fatally undermined by APP 8.2, coupled with s16A, which provides at least nine separate grounds on which a data exporter can be exempt from even the theoretical liability/'accountability' of APP 8.1.

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 8.2(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 to remedying this defect in the current Bill 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.

Submission 47: The solution to the problems of APP 8 is to delete the words '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.

The second exception is where there is consent based on explicit notice that the exporter accepts no liability ('accountability') for whatever happens overseas (APP 8.2(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.

Submission 48: Any exception based on explicit notice that the exporter accepts no liability must include an express requirement for the organisation to explain the risk involved.

Another exception is where Australia is a party to some international agreement that relates to information sharing (APP 8.2(e)) – 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.

Submission 49: The exceptions for international agreements should be deleted as they will encourage policy laundering.

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.

Submission 50: The two key changes required to APP 8 are: (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 – Weaker protection in the private sector

The existing restrictions on the private sector using Commonwealth government identifiers (NPP 7) have been strengthened by extension to the use of State or Territory government identifiers. However, APP 9 only applies to the private sector (organisations), and the Use and Disclosure principle (APP 6) now does not apply to an organisation (private sector) in relation to government related identifiers. Previously, both principles applied. In contrast, the government identifiers principle will not apply to the use of such identifiers by government agencies, but APP 6 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 APP 9.

Submission 51: APP 9 should apply to all situations where the previous NPP 7 applied.

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.

4 Credit Reporting: A major loss of financial privacy for what return?

Schedule 2 of the Bill is a major re-write of the Credit reporting provisions in the Act (Part IIIA) which have been in effect, largely unchanged, since 1991.

It is important to understand that the credit reporting system (both now and under these amendments) is a statutorily authorised intrusion into individuals' privacy, and in effect a 'licenced' exception to the normal operation of the default private sector Privacy Principles in the Privacy Act (now the NPPs, and proposed APPs).

There has never been anything to stop lenders asking applicants for loans about their existing commitments, and making evidence of such commitments (e.g. bank references) a condition of a loan. Lenders do not of course want to do this – it would be costly and 'annoy' many applicants. The government decided, in 1989, to insert Part IIIA into the Privacy Act to allow, and regulate, a system of 'no choice' exchange of credit reporting information. This was justified on the basis that the public interest in the efficiency of the consumer credit market outweighed the inherent loss of personal privacy involved in a system of centralised credit reporting.

It is important to understand this context because the proposed amendments involve the 'licensing' of a significant further intrusion into individuals' privacy, with no choice (other than not to apply for credit at all, including telephone or electricity accounts – which is unrealistic in the modern economy). Any suggestion that lenders and utility companies have a 'right' to centrally held credit reporting information should therefore be dismissed – the credit reporting system is a privilege, and it is incumbent on industry to justify any extension, and appropriate for the system to be very tightly regulated.

More comprehensive reporting

Comprehensive credit reporting will give credit providers access to additional personal information to assist them in establishing an individual's credit worthiness. As the Explanatory Memorandum states:

> "This means a limited number of additional kinds of credit related personal information about individuals are permitted in the credit reporting system. The five new kinds of personal information (also known in the industry as 'data sets') are:
>
> - the date the credit account was opened
> - the type of credit account opened
> - the date the credit account was closed
> - the current limit of each open credit account; and
> - repayment performance history about the individual." (EM p3)

It is asserted that:

> "The additional personal information will allow credit providers to make a more robust assessment of credit risk and assist credit providers to meet their responsible lending obligations. It is expected that this will lead to decreased levels of over-

> indebtedness and lower credit default rates. More comprehensive credit reporting is also expected to improve competition and efficiency in the credit market, which may result in reductions to the cost of credit for individuals." (EM p3)

Overseas research shows that access to more personal data leads to an overall increase in the level of consumer credit. Lenders will use this information to enable more profitable lending. While this often aligns with lending that benefits the individual, this is not always the case. We continue to have concerns that the increase in levels of consumer credit will have a detrimental effect on some consumers – but the overall impact will depend on the detail of this increase – which consumers will receive the additional credit and what types of credit products will be offered. We welcome the imposition of 'responsible lending' conditions for participation in the credit reporting provisions, which protects consumers against the more blatant irresponsible lending practices, but this does not mean that consumer vulnerabilities will not be exploited to provide credit which is not in the consumer's best interests. We draw the Committee's attention to a fact sheet relevant to this issue from Consumer Action Victoria[5].

These additional data sets represent a major increase in the level of statutorily authorised intrusion into the financial affairs of most Australians. The APF has consistently argued that this move towards more comprehensive reporting is unnecessary and undesirable, especially in the context of recent history of irresponsible lending, contributing to the global financial crisis of 2008-09. We suggest that the government's decision to only allow a more limited extension than the industry would have liked validates many of our concerns.

The Explanatory Memorandum includes a lengthy Regulation Impact Statement (pp 14-29 of the EM) devoted to the credit reporting reforms. The main conclusion of this RIS is that :

> "The introduction of more comprehensive credit reporting in the form of the additional five data sets will provide consumer credit providers with the opportunity to access enhanced information to establish an individual's credit worthiness. It is expected that this will allow more robust assessments of consumer credit risk, both in the market as a whole and in relation to individual applications, which can assist responsible lending and potentially lead to lower consumer credit default rates. The economic benefits to industry and individuals alike outweigh the reduction of privacy protections to these categories of personal information." (EM p29)

In this context, we draw the Committee's attention to the Comprehensive Reporting pilot currently being undertaken by most of the major lenders and one of the major Credit Reporting bodies - Veda. This pilot involves a massive database of credit information about most Australian borrowers, carefully de-identified to avoid breaching the current Privacy Act controls. The database is being used to model the likely effect of comprehensive reporting. It has already produced both valuable new information

[5] http://www.consumeraction.org.au/downloads/FactSheet-creditreportingandresponsiblelendingDec08.pdf

about the 'profile' of consumer credit in Australia, and preliminary findings about the possible changes in lending that could follow the availability of the five extra data sets.

Consumer groups and the Privacy Commissioner were consulted about the pilot, and could see value in the exercise, provided it was strictly managed. However, the full value will only be realised if the findings are available to inform the development of public policy, including this Inquiry. We believe that at least some of this valuable information could be made public, without insuperable obstacles of commercial confidentiality. We urge the Committee to seek a summary of the findings from Veda (which is administering the pilot), as we believe they are relevant to consideration of the merits of the proposed changes – specifically in relation to the claims made about the predictive value of repayment history in section 4.2.3.1. of the RIS in the EM.

Submission 52: The Committee should seek access to relevant findings of the current Comprehensive Reporting pilot.

We believe that new information, together with changing circumstances in relation to the financial sector since the ALRC was conducting its review in 2005-08, warrant a re-assessment of the balance between the alleged benefits of comprehensive reporting and the inevitable major loss of financial privacy for all Australians.

Submission 53: The Committee should seriously consider, in the light of all available evidence, whether the provisions of the Bill providing for more comprehensive credit reporting should be approved.

Outstanding concerns with the Credit Reporting provisions

We note that the Consumer Action Law Centre has made a submission to this Inquiry raising concerns about four aspects of Schedule 2. These relate to:

- Serious Credit Infringements: definition of Serious Credit Infringement at proposed section 6(1) - a preferable solution has been proposed jointly by Veda Advantage and consumer advocates (including APF).

- Requests to correct information: While welcoming the removal in proposed section 20U of the two-step complaint process which was in the previous exposure draft, the provision still does not meet the standard recommended by the Australian Law Reform Commission in *For Your Information* and accepted by the Government.

- Complaint handling: While strongly supporting the intent behind the complaint handling process at proposed section 23B, concern that the obligation may ultimately be counter-productive – an alternative is recommended.

- Hardship variations: Any approach to listing hardship variations should be designed to ensure consumers are not discouraged from approaching their lenders and requesting hardship variations when needed.

APF has been an active participant, with CALC and other consumer groups, in discussions with Veda and with ARCA over the last few years. Rather than repeat the CALC arguments, APF endorses their submission on these matters in full.

Telecommunications and other Utilities

We note that ACCAN has made a submission to the Committee concerning the special circumstances of telecommunications consumers in relation to the credit reporting system. We are aware that ACANN's concerns are shared by financial counselling NGOs. APF defers to ACCAN's expertise in this area, and endorses their recommendations 3-7. We understand that similar difficulties are experienced by customers of other utilities such as energy suppliers, and consideration should be given to making the telco amendments suggested by ACCAN apply to all utilities.

Submission 54: The Committee should recommend that the government give serious consideration to the amendments suggested by ACCAN in recommendations 3-7 in their submission, and also to applying these amendments to all utilities.

Location of provisions – Act vs Regulations vs Code

Throughout the lengthy consultation on reform of the credit reporting provisions, APF together with other NGOs has been concerned to ensure that as many as possible of the key provisions are 'locked in' in the legislation itself. While Regulations can be a useful mechanism in limited circumstances, they are notoriously weaker than statute – being more easily changed and typically subject to much less scrutiny by Parliament than primary legislation.

We are even more concerned to ensure that important provisions, and safeguards, are not left to the proposed Credit Reporting Code, to be approved by the Information Commissioner. However widely the Information Commissioner consults in the preparation of a Code (see comments on Part IIIB below), there is a clear 'democratic deficit' in this process. Experience with the similar role of the Privacy Commissioner under Part IIIA is that industry pressure can lead to Code provisions which undermine the effect of the Act. An example is the Privacy Commissioner's interpretation of the permissible timing of notice of default listings. While we accept the role of a Code in fleshing out some of the operational details, we do not believe it is the place for any significant threshold provisions.

To the extent that some matters are proposed to be dealt with in Regulations, it is important that the Parliament is able to see draft Regulations whilst debating the Bill – otherwise the interrelationship, and adequacy of the overall regulatory package, cannot be properly assessed.

We have identified the following provisions where Regulations are proposed – some of them are very significant determinants of the scope and effect of the regulatory scheme:

- Additional criteria for use and disclosure of CRI by CRB – proposed s20E (3)(f)
- Additional requirements for disclosure of CI by CP to CRB – proposed s21D(3)(c)
- Additional uses and disclosures for CEI by CPs – proposed s21G(2) (d) and (e) and (3)(f) & g)
- Definition of **credit reporting body** – proposed s6P(4) allows for exclusions by regs
- Threshold $ amount in definition of **default information** – proposed s6Q
- Additional detail for definition of **repayment history information** – proposed s6V(2)
- Definition of **credit provider** – proposed s6G(1)(d) - provides for additions and s6G(5) and (6) for prohibitions

- Definition of **credit reporting body** – proposed s6P provides for agencies to be CRBs

Some of these matters would have a profound effect on the scope and effect of the regulatory scheme for credit reporting.

Submission 55: The Committee should seek confirmation of this list and insist that draft Regulations be made available for consideration alongside the Bill.

Similarly, the Committee should seek a clear statement of what matters it is proposed be left to the proposed CR Code.

Those we have identified so far are:

- Pre-screening – s20G(2)(f)
- Means of access – CRVs s20R(4) and CPs s21T(4)
- Additional notification requirements for CPs – s21C(1)
- Contents of notice by CPs – s21P(2))

Submission 56: The Committee should seek confirmation of this list and clarification of the likely scope of any Code provisions dealing with these matters, for consideration alongside the Bill

Definitions concerning credit reporting

Various concepts are either new, revised or defined in the Act for the first time – 'credit'; 'credit information' (CI); 'credit reporting information (CRI) 'commercial credit'; commercial credit related purpose; 'consumer credit'; consumer credit related purpose'; consumer credit liability information' (CCLI); credit eligibility information' (CEI); 'credit worthiness'; 'CP derived information' (CPDI); 'CRB derived information' (CRBDI); 'credit reporting business' (CRbus); 'credit reporting body' (CRB), and 'credit provider' (CP) (definitions either in s6(1) and/or in new ss. 6G-6V).

This hardly constitutes the 'simplification' desired by all parties and promised in the EM, and we submit that the scheme is now effectively too complex to be readily explicable, posing a serious risk of non-compliance and/or inability of consumers to effectively exercise their rights. At the very least the definitions need careful review to ensure they 'work' as intended.

Submission 57: The Committee should give serious consideration to whether the credit reporting provisions in the Bill (Schedule 2) are simply too complex and should be sent back to the government for a better attempt at the simplification recommended by the ALRC and widely supported

We note that the definition of 'consumer credit' is different from that in the recently introduced National Credit Code6 This is unhelpful. If intentional, the reasons need to be explained.

---

6 http://archive.treasury.gov.au/documents/1523/PDF/ED_regulations_1_National_Consumer_Credit_NCC_Regulations_2009.pdf

Submission 58: The Committee should request an explanation from government as to the justification (if any) for the discrepancy between the two definitions, and why this confusion could not be avoided with an alternative term.

A new concept of 'Identification Information' (II) is defined in s6(1) and used in the definition of credit information (proposed s6N) – definition of II is 'context specific' to credit reporting and it would be better not to introduce a term into Australian law which may be taken out of context and used as a precedent in other contexts –

Submission 59: The term 'Identifying Information' should be replaced with Credit Identifying Information'.

A new concept of 'access seeker' is defined in proposed s6L(1) – and this seems appropriate as used in proposed s20R and s21T. However, the prohibition on credit providers etc being an access seeker effected through s6L(2) is clumsy and potentially ineffective – an individual will not be in a position to know that they 'must not authorise' a Credit Provider or one of the other specified types of entity.

Submission 60: The prohibition on Credit Providers et al being access seekers must apply directly to these entities, rather than relying on individuals knowing that they can (must?) refuse to authorise such entities.

We note that ACCAN has made a submission to the Committee recommending an amendment to the 'exception' in proposed s6L for the National Relay Service. ACCAN makes the valid point that there are other providers of similar services to the NRS, and they propose a further conditional exception, with the Minister able to determine other relay services and the Information Commissioner to maintain a register. We support this amendment.

Submission 61: The Committee should recommend the amendment of proposed s6L suggested by ACCAN in recommendations 1 and 2 in their submision.

'Internal management .... directly related to the provision or management of ... credit' (as used in proposed s21H) is undefined – this term is too loose and therefore open to abuse. We understand that industry may have its own definition of this but it is vital that it should be more narrowly defined, since a broad interpretation could fatally compromise the intention of the legislation to strictly limit uses of credit reporting information. The financial counselling NGOs should be invited to suggest specific wording.

Submission 62: The Committee should recommend that the government negotiate a narrower definition of 'internal management ...' for the purposes of the credit reporting regime.

The exclusion of real estate agents, general insurers and employers from the definition of 'credit provider' in proposed s6G (5) is welcome but the precise effect is unclear. The past intention was been to deny them access to CRI altogether – we submit that the Committee should seek assurances that is this still the effect.

Specifically, the use of credit reporting for assessing potential tenants should be prohibited, as businesses other than real estate agents can and do undertake the management of rental properties (including landlords).

Submission 63: The Committee should seek assurance from the government that the use of credit reporting information by real estate agents, general insurers and employers is effectively precluded by proposed s6G(5)

Submission 64: The use of credit reporting information by any person or body for the purpose of assessing potential tenants should be expressly prohibited.

Division 2 – Credit Reporting Bodies

Overseas transfers

In proposed s20B (the equivalent of APP1), there is no equivalent to APP 1.4 (f) and (g), and there is no equivalent at all to APP8, both concerning overseas transfers. It is not clear that 'Australian link' provisions (which effectively prohibit disclosure of information from the credit reporting system to foreign credit reporting bodies or foreign credit providers would also regulate the disclosure of credit information to other overseas recipients for other purposes. Any such disclosures would expressly not be covered by the APPs.

Submission 65: The Committee should seek assurances that the Bill would not create a gap in which some overseas disclosures of information from the credit reporting system would be unregulated.

We question why it is necessary to provide for extra uses/disclosures to be authorised by Regulation (proposed ss. 20E, 21DE and 21G) given that this is not provided for in the equivalent APP 6. Why is this flexibility considered appropriate only for credit reporting? In our view, the necessary uses and disclosures were thoroughly canvassed during the ALRC and subsequent consultation processes and it should be possible for the legislation to contain a definitive list. The EM gives assurances that any proposed regulations would be the subject of consultation, but this is both unreliable and an insufficient safeguard.

Submission 66: The Committee should seek an explanation as to why it is necessary to provide for extra uses/disclosures of credit reporting information and credit eligibility information to be authorised by Regulation, when no such flexibility is considered necessary in the APP regime.

Direct marketing and pre-screening

Proposed ss 20G-20J place some welcome limits on the use of credit reporting information for direct marketing and pre-screening. There are however two remaining concerns.

Section 20G(5) provides for an 'opt-out' from the use of credit information for pre-screening but this will not work well as there is no direct relationship/contact between individual and a CRB – it is unrealistic to rely on individuals 'finding' a CRB to opt-out – they must be given the opportunity via their direct relationship with a Credit Provider. Section 20G(2) does after all purport to regulate pre-screening by a CRB *on behalf of* a CP. Consistent with the general approach to direct marketing regulation under not just the Privacy Act but also the *Spam Act 2003* and *Do Not Call Register Act 2006*, credit providers should be expressly required to offer a clear 'opt-out' offer in all relevant communications, including loan offers sent after any pre-screening.

Submission 67: We submit that a specific and detailed obligation on Credit Providers to offer an opt-out from pre-screening should be included in Division 3 of the revised Part IIIA.

In proposed s20G(7) (and elsewhere), there is provision for 'written notes' of particular actions. It is unclear as to how this would be implemented in electronic records and/or automated systems, and the value is also unclear; i.e. who gets to see them in what circumstances – or are they just for post-facto audit?

More generally, the term "written note" is used throughout the Bill – it would be clearer if the requirements were for a "record" rather than a "note", and there was an express obligation to retain the records. It is unclear as to whether these notes/records will be included in the credit report so that the individual can access them, and if necessary challenge them. We believe they should be.

Submission 68: The term 'written note' should be replaced with 'record' throughout the Bill, and an obligation added to retain such 'records'.

Submission 69: In proposed s20G(7) the "note" (record) in relation to access for pre-screening purposes should expressly be required to be made available to the individual whenever s/he obtains a copy of the credit report.

Given the limited amount of data that can be used in pre-screening, it appears that in allowing the CP to determine the eligibility requirements, some CPs may only choose to exclude people with no defaults; more than one default etc. It would also appear possible for a CP to screen out those without defaults.

Also, if pre-screening is to allow offers to be made to consumers who have defaults, we would question the benefits (if any) of pre-screening in contributing to responsible lending – see our general comments above about the overall public benefit in allowing more comprehensive reporting.

Submission 70: The law should only allow pre-screening to use default, SCI, judgment and bankruptcy information, and should only be used to filter out negative information – it should not be lawful to filter out people who don't have defaults.

Ban periods for suspected fraud by a third party

Proposed s20K provides for an individual to trigger a 'ban period' – this is welcome, but there should also be provision for action by CRBs becoming aware of possible third party fraud by other means, which is arguably much more likely than an individual's report. In such cases CRBs should be required to consult the individual about the imposition of a ban period.

The ban can be triggered by an individual's 'reasonable belief' that they (may) have been the victim of fraud (ss(1)(b)), but it is not clear whether this 'reasonableness can be assessed or challenged by the CRB (we note that the EM seeks to re-assure on this matter but we are not convinced that the provision is clear enough to prevent unhelpful interpretations.

We note that for the ban period to be extended it is the CRB which must have the reasonable belief (ss(4)(c)), but that there is no obligation on the CRB to make reasonable enquiries.

Submission 71: There should be an obligation on the CRB to make reasonable enquiries about alleged fraud in forming their 'reasonable belief' to justify extension of a ban.

Proposed subsection (4)(d) gives too much discretion to the CRB in relation to extension of the ban period – there needs to be some mechanism for individuals to appeal decisions they disagree with – e.g. to the Information Commissioner.

Proposed s20K(2)(a) seems too broad – why would an individual have consented in writing to disclosure under the whole CRB Division and when would this be directly relevant to a specific instance of suspected fraud? If this provision is only intended to allow an individual who has initiated a ban to lift it before the default 21 day period has elapsed (an important right for innocent fraud victims), then it should be more narrowly constructed. It should also be possible for an individual to authorise a specific disclosure while leaving an overall ban in place – this could be of critical importance to an individual's financial situation.

We envisage that any potential CP who saw there was a ban would wait until the ban was lifted before providing credit, or at least make appropriate enquiries of the individual, and/or other parties.

Submission 72: Some inconsistencies and uncertainties in the operation of the 'ban' provision need to be resolved. This may require amendments. The Bill should provide for CRBs to initiate consultation with an individual about a ban whenever they become aware of possible fraud, for appeal rights, and for the ability to selectively authorise disclosures while a ban is in place.

Government issued identifiers

Proposed s20L is the equivalent of APP9. As with APP9, it is unclear what 'adopt ... as its own identifier' means in practice. If it would potentially apply to State and Territory Drivers Licence Numbers (DLN) , would the inclusion of DLN in the definition of 'identification information' in s6(1) invoke s20L(2) to allow their use?

Submission 73: The Committee should seek clarification of the effect of proposed s20L.

De-identified information

Proposed s20M provides for rules relating to the use of de-identified information to be made by the Information Commissioner, but leaves too much discretion - the IC ('may... make ; '... any Rules ...")

Submission 74: There should be an obligation on the Commissioner to make such rules.

Access

Proposed s20R(5) provides for only one free access request per year. This limitation needs justifying, and must allow for more than one free when requests are associated with dispute resolution etc.

Submission 75: The Act should allow for more than one free when requests are associated with dispute resolution.

Proposed s20S is a separate correction obligation when the CRA becomes aware by other means (separate from correction 'on request' which is addressed in proposed s20T). This separation is acceptable in principle but there is no justification for the

'notice of correction' obligations in proposed s20U to only apply to correction requests initiated by the individual under s20T and not to other corrections under s20S.

Submission 76: Notice of objection obligations in proposed s20U should apply to corrections under both s20T and s20S.

Unlike in the equivalent APP 13, there is no provision for an' associated statement' if a correction request remains disputed. Also, we have concerns about exception in s20U(4) where it is 'impracticable' for a CRB to give notice to a recipient of credit reporting information that the information has been corrected. There is similar wording in some other sections. We can't understand why it might be impracticable for a CRB to record 'associated statements' and to provide both corrected information and 'associated statements' to a recipient if it has appropriate systems in place. Individuals should not be deprived of rights as a consequence of technological choices or business process decisions – it is up to the industry to devise means of flagging corrected or disputed information and bringing it to the attention of users.

Submission 77: There should be an obligation on CRBs to add an 'associated statement' to a individual's record where a correction dispute remains unresolved, as applies under APP13.

Proposed s20T incorporates a welcome time limit (ss(2) and requirement to consult (ss(3). However, there is no time limit where the CRB is not satisfied and needs to consult. The provisions are weaker than the ALRC's recommendation 59-8 which was to require a CRB to delete or correct challenged information if the CP did not either substantiate the information or refer the dispute to a recognized EDR scheme within 30 days.

Submission 78: ALRC recommendation 59-8 should be implemented in full.

Division 3 - Credit Providers

Proposed s21C(1) leaves the detail of additional content of the required notice (beyond what will be required under APP5 and the name of the CRB) to the proposed Code. This is a very important matter and we submit that more detailed content requirements should be included in the Act, as well as more specific requirements as to timing of notice in the credit reporting context, which has been a contentious issue under the existing scheme.

There appears to be a major gap in the scheme in terms of notification of individuals close to the time that a CP lists default or SCI information with a CRB – the legislation appears to allow a CP to rely on the initial notice given at the time the loan was taken out, to warn borrowers of the risk of listing.

This is the case with the current laws, although the PC has allowed this notice to be provided just prior to listing, even if there was no notice provided at the time the consumer first provided information to the credit provider.

It is not appropriate for this information to be provided only once – whether this is at the time that initial information is collected or just prior to a default listing being made.

Submission 79: The Bill should require that consumers are notified at the time their personal information is collected (at the time they apply for credit) and it should also

expressly require notice within a reasonably short time period before any listing, irrespective of what notice has been provided earlier; e.g. when the loan was taken out.

Disclosure of credit information to a credit reporting body

Proposed section 21D has a very confusing construction, mixing up type of information, limits and conditions

Submission 80: Clause 21D should be re-drafted to follow a more logical and easily explained sequence of 'type of information' , then limits, then conditions.

Further to our general concern about Regulations, expressed above, we submit that the Committee should ask what if any Regulations under s21D(3)(c)(iii) are proposed from outset?

In s21D (3)(d)(ii), 'reasonable period' is too subjective and leaves it to the judgment of the CP – we submit that the Act should specify a minimum – we suggest 14 days.

Submission 81: Clause 21D (3)(d)(ii) should specify a minimum period

We submit that there should be a fairness provision in s21D that requires CPs to consider any special hardship circumstances, such as hospitalisation, natural disaster, bank error; etc, that they are aware of, before listing defaults or adverse repayment history, permitted by (3)(d) and (c) respectively.

Submission 82: There should be an obligation on Credit Providers to consider hardship factors and a borrower's circumstances before listing any defaults or adverse repayment history.

Use or disclosure of credit eligibility information

In proposed s21G(3), ownership should not override the purpose limitations – individuals typically have no understanding, or interest, in corporate structures and their reasonable expectation is that their dealings are with the entity with whom they are transacting – uses and disclosures by and to 'related bodies corporate' should be subject to the same rules as for other third parties. The limits placed on related bodies corporate by proposed s22D do not adequately address this concern. This is a more general criticism of the Privacy Act's approach to related bodies corporate but has particular significance in the context of credit reporting.

Submission 83: Disclosures to related bodies corporate should be subject to the same rules as for other third parties.

In proposed s21G(3)(e)(ii) it is not clear why 'or credit reporting body' is included, since this section is entirely about an obligation of credit providers?

Submission 84: The Committee should seek an explanation of the inclusion of 'or CRB' in proposed s s21G(3)(e)(ii)

Direct marketing and pre-screening

There are no direct marketing or pre-screening controls applying directly on CPs – all are via the CRB obligations in Division 2 – as we have argued above this is unsatisfactory – individuals will not routinely have contact with a CRB to be offered 'opt-outs' - and may leave other loopholes..

Submission 85: Division 3 should contain appropriate versions of the Division 2 controls on direct marketing and pre-screening, applying expressly to credit providers

Permitted use of credit eligibility information in relation to the individual

In the table under proposed 21H(b), one permitted purpose (Item 5) is for the purpose of 'assisting an individual to avoid defaulting on his/her obligations'. We have concerns about the ability of a CP to obtain ongoing access to a customer's credit report under this provision. It is unclear how this might be used by a CP. If it is to allow a CP to reduce a credit limit then it should be limited to that. If this provision is unchanged, there is a need to have additional audit processes to monitor specifically how this information is used.

We have concerns that in a similar way to "internal management purposes" this could be used quite broadly. For example this could include making an offer to refinance or even to offer additional finance. We have concerns about how broader uses could be effectively monitored, but this use should be restricted to reducing a credit limit or refusing any extension of further credit.

Submission 86: The purposes of "assisting an individual to avoid defaulting on his/her obligations" should be defined to either deciding to reduce a credit limit or refuse any extension of further credit.

Disclosures between credit providers

In Proposed Section 21J(1)(a) – 'a' particular purpose is too loose/permissive, as it could be read, in conjunction with (b) as 'any' particular purpose to which the individual has consented. Given the common practice of requiring consent as a condition of financial transactions, this opens the door for disclosures to other credit providers which are wholly unrelated to either the particular transaction the individual has entered or the limited exchange of credit reporting information allowed under this regime.

Submission 87: The Bill should be amended to close the potential loophole created by the wording of proposed s21J(1)(a)

Proposed s21J(2)(a)(i) appears to mean that no consent is required for credit assessment – we submit that the implications of this are very significant and need to be explored by the Committee. Under the current Act (Part IIIA), consent is required. We have been critical of this as consent is effectively mandatory as a condition of a loan application – it is not freely given and cannot be revoked. In such circumstances we have argued for 'notice and acknowledgement' in place of consent, as a more accurate reflection of what is actually happening. If the effect of proposed s21J(2)(a)(i) is to remove the requirement for written consent then we submit that it needs to substitute an express requirement for notice and acknowledgement .

Submission 88: The Committee should seek clarification of the effect of proposed s21J(2)(a)(i). If the effect is to remove the requirement for written consent for credit assessment then an express requirement for notice and acknowledgement should be inserted

In proposed s21K(3)&(4), the guarantor consent requirement seems less onerous than for borrower i.e. it need not be in writing) – we would expect it to be the same or tougher.

Submission 89: The Committee should seek an explanation of this provision and failing a satisfactory response, the guarantor consent requirements should be the same as that of borrowers.

We don't understand proposed s21M(2)(d)(ii) , as it seems to suggest that a CP might not hold payment information relating to an overdue payment to the CP, which seems improbable?

Submission 90: The Committee should ask for a clarification of the intent and need for proposed s21M(2)(d)(ii)

In relation to proposed s21V(1)(b), in practice almost all consumers who complain to CPs do so because of information that has been reported to a CRB by a credit provider, so it shouldn't be necessary for the CP to "hold at least one type of personal information" - and it would be unfair if any consumer had to show that the CP did. The key issue here is that the CP has reported the information to the CRB.

Submission 91: Clause s21V(1)(b) should include the additional words (in CAPS here) " the provider holds OR HAS REPORTED TO A CRB at least one kind of the personal information referred to in paragraph (a)."

Submission 92: In Section 21W(3)(c)(i), the notice of correction should expressly include the EDR scheme contact details.

Division 4 – Affected Information recipients

There appear to be no limits placed on debt collectors, who are permitted to receive credit eligibility information from credit providers (under proposed s21M), but do not fall within the definition of 'affected information recipient' in s6(1) to which the limits in this Division apply. The use of credit reporting information by debt collectors has been a major issue under Part IIIA and we submit that strict controls are required.

Submission 93: Secondary use and disclosure limits need to be placed on debt collectors, preferably by including them within the definition of 'affected information recipient' and if necessary with specific provisions within Division 4 Subdivision B

Division 5 – Complaints

In relation to proposed s23B(5), we question what the effect would be if an EDR scheme has different rules/time periods under its existing constitution and operational procedures?

Submission 94: The Committee should seek an explanation of what is expected to happen if a recognised EDR scheme has different rules/time periods in its constitution and operating procedures from those in this proposed section.

Other credit reporting matters

Submission 95: There should be a requirement that if a CP goes into liquidation, or otherwise ceases to be a member of a recognized EDR scheme, all listings made by that CP on a CRB database should be removed. It is not acceptable for listings to remain without a mechanism for challenge.

5 Codes: Low priority, useful additional protection

Division 2 – Registered APP Codes

The existing general Code provisions in the Act – introduced with the Private Sector Amendments in 2000 – have manifestly failed. There have only been four Codes registered since 2000, and two of those have subsequently been withdrawn and de-registered.

The ALRC recommended that outside the credit reporting jurisdiction, Codes should only provide guidance or standards on the default Principles (ALRC Rec 48-1). The government proposes that in addition Codes may also introduce additional binding obligations, provided they deal only with information privacy.

The Bill does also now make it clear that Codes may not derogate from the APPs, and removes the unhelpful, and largely unused, option of a separate Code Adjudicator. Codes may deal with internal complaint processes but cannot tamper with the external complaint provisions of the Act.

The Bill does also introduce two new options for Code development – at the request of the Commissioner, and by the Commissioner. These options potentially allow the Commissioner to initiate a process for imposing additional binding information privacy obligations on APP entities, where this is justified. We see this as a useful addition to the toolkit of privacy protection, particularly as Codes can apply, for the first time, to Commonwealth agencies. The value of the Commissioner initiated Code provisions will of course only be realised if the Commissioner has both the will and the resources to utilize them.

Submission 96: The inclusion of a revised provision for binding Codes applying to APP entities will be a useful addition to the Act, and the changes from the existing Part IIIAA remove most of the weaknesses of the current Code provisions, while strengthening them significantly.

Section 26B includes a very confusing relationship between commencement and dual registration – on Commissioner's Code Register and on Register of Legislative Instruments. APP Codes are not legislative instruments until/unless registered (*on both registers?*)

Submission 97: The Committee should seek clarification of the relationship between the two 'registrations' required for Codes and the implications for commencement

There is one questionable provision in Section 26C – ss (2)(b) allows Codes to cover acts and practices exempt under s7B(1),(2) or (3). Section 7B(1) is individuals (2) is Commonwealth contracted service providers, (3) is employee records. Given that these inclusions can only be voluntary (the Commissioner can't impose these 'extras') only (3) makes sense – individuals or contractors are hardly likely to volunteer to be subject to the Act. It is disappointing that the Bill fails to provide for voluntary inclusion of a range of other exempt matters by organizations, and for any such matters by agencies.

Submission 98: The Bill should be amended to allow Code developers to voluntarily include any exempt matter.

The procedural provisions about the development, approval, registration etc of APP Codes are largely modelled on the existing processes in Part IIIAA. While these appear generally acceptable, we note that there have been some problems in practice with the operation of Part IIIA, particularly in relation to adequate notice of and consultation on code development, variation and revocation. We reserve judgement on whether the procedural aspects of the Code provisions applying to APP Codes in the proposed Divisions 2 & 4 of Part IIIB will work well in practice.

Division 3 – Registered Credit Reporting (CR) Code

In the section of this submission on the new credit reporting provisions (replacement Part IIIA) we have already stated our concern about significant matters being left both to Regulations and to the proposed CR Code. We listed some matters which we have identified as being left for the CR Code, and recommended that the Committee seek a comprehensive list, and better justification for these matters not being addressed in the Bill itself.

We welcome the provision that there can only be a single CR Code, and confirmation that the CR Code will not be able to derogate from the provisions of Part IIIA, rather only 'set out how one or more of the credit reporting provisions are to be applied or complied with' (EM p4). The procedural provisions about the development, approval, registration etc of the CR Code are modelled on those applying also to APP Codes, and to a largely also on the existing processes in Part IIIAA. While these appear generally acceptable, we note that there have been some problems in practice with the operation of Part IIIA, particularly in relation to adequate notice of and consultation on code development, variation and revocation.

We are aware that the Credit Reporting Industry, through its representative body ARCA, has already embarked on a code development process in anticipation of the amendments, and have been involved in consultations. This process may need to be adjusted in light of the detailed provisions which have only just been made public. We reserve judgement on whether the CR Code provisions in the proposed Division 3 of Part IIIB will work well in practice.

Item 9 in Schedule 3 is a consequential amendment that confirms that the term 'credit provider' has a different meaning - including mortgage insurers and trade insurers – in some parts of the Act (including Pt IIIB – Codes) but not in the main credit reporting Part IIIA (where insurers are expressly dealt with differently). It has been and will continue to be very unhelpful and confusing to have two different definitions of CP in different contexts.

Submission 99: The term 'credit provider' should not have two different meanings in different, but related parts of the same Act

Division 4 – General Code Matters

Proposed s26U (4) allows the Commissioner to charge fees for copies or extracts of Codes Registers. This is wholly unacceptable – Codes will form part of privacy law, and must remain both readily accessible and free. S26U(3) requires publication on the Commissioner's website but it is essential that Codes also be available to individuals without online access.

Submission 100: The Commissioner should be required to make access to registered Codes easy and free, including reasonable off-line access.

For further information please contact:

Graham Greenleaf [redacted] or

Nigel Waters [redacted]

Board Members
Australian Privacy Foundation

APF Web site: http://www.privacy.org.au

Please note that APF's preferred mode of communication is by email, which should be answered without undue delay. APF does not have an organisational postal address. If postal communication is necessary, please contact the person named above to arrange for a postal address.

List of specific Australian Privacy Foundation submissions (embedded in section headings and with page references to body of overall submission)