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

Implementing privacy principles in Credit Reporting

Submission to the Australian Law Reform Commission
on the Review of Privacy Issues Paper 32: Credit Reporting Provisions

Nigel Waters

Nigel Waters
Principal Researcher, Interpreting Privacy Principles Project
Cyberspace Law & Policy Centre, UNSW Faculty of Law

31 March 2007

Research for this submission is part of the Interpreting Privacy Principles Project, an Australian Research Council Discovery Project

Contents

Introduction

Structure of Submission

This submission does not directly follow the order of chapters in *Issues Paper 32*. Because our emphasis is on a comparison of the credit reporting provisions and the National Privacy Principles, I have adopted a somewhat different structure. However I have referenced the submission to the relevant paragraphs and Questions in IP 32.

I have not made submissions on quite a few of questions asked in the Issues Paper, not because of their lack of importance but because I have limited myself to those issues and questions which relate to interpretation of privacy principles, and not generally to those which go to wider public policy issues. I am otherwise in general agreement with the submissions made by the Australian Privacy Foundation, to which I contributed, and by other consumer groups with practical experience of the credit reporting provisions in operation.

Background – the iPP Project

Research for this submission has been undertaken as part of a Discovery project funded by the Australian Research Council, 'Interpreting Privacy Principles'. The home page for the project, and other publications relating to the project, are at <http://www.cyberlawcentre.org/ipp/>. The *iPP Project* is based at the Cyberspace Law & Policy Centre at UNSW Law Faculty. The principal objective of this research is to conduct over the course of the project (2006-09) a comprehensive Australian study of (i) the interpretation of information privacy principles (IPPs) and 'core concepts' in Australia's various privacy laws, particularly by Courts, Tribunals and privacy regulators; (ii) the extent of current statutory uniformity between jurisdictions and types of laws, and (iii) proposals for reforms to obtain better uniformity, certainty, and protection of privacy.

Concerning the first element, a small but rapidly growing body of cases has developed in Australia over the last few years. Around a hundred Tribunal decisions, a similar quantity of mediated complaint summaries, and relatively small number of relevant Court decisions have become available. There has been little systematic analysis of this material. The relative scarcity of Australian interpretative materials means that the objective necessitates consideration of the interpretation of similar IPPs and core concepts in the privacy laws of other Asia-Pacific countries (particularly New Zealand, which has the largest quantity of reported cases) and European jurisdictions. The iPP Project, as it develops this analysis, will aim to make further inputs into the ALRC's review and similar privacy reform projects at State level.

In relation to the credit reporting provisions of the Privacy Act, there are few reported cases. There have been no formal complaint Determinations by the Privacy Commissioner involving Part IIIA or Code of Conduct breaches, and no court actions. Commissioners have been systematically publishing anonymised complaint case notes since 2002, and before that reported in varying degree of detail on credit reporting compliance in Annual Reports. I have cited case notes where relevant to the analysis in this submission.

I have also made reference where it seems relevant to the Credit Reporting Privacy Code[1] under the New Zealand Privacy Act.

[1] Revised to incorporate amendments, March 2006 – at http://www.privacy.org.nz/filestore/docfiles/49179009.doc

Scope of the Review

I submit that it is impossible to achieve the objectives of credit reporting regulation without also addressing the *use* of the personal information collected and reported by credit providers. The Privacy Act currently already does so to some extent, but neither the Privacy Act nor credit laws deal with the ultimately critical issues of how the information can be used in credit assessment and scoring. There is no regulation of the relevance, proportionality, completeness or steps taken to verify information that feeds into lending decisions.

Many of the concerns about the use of consumer credit information relate to lending practices – a policy arena in which there is already a major debate between financial industry and consumer groups with expertise in financial services about responsible vs reckless lending. While I understand that this wider policy area may be seen prima facie as going beyond the terms of reference of the ALRC Review, I suggest that the wider definition of 'report' for the purposes of credit provider obligations (section 18N(9)) already places credit assessment and lending practices within the scope of the Privacy Act jurisdiction, and therefore legitimately within the scope of the Review.

The existing regime already regulates much more than just information held by credit reporting agencies (CRAs); it also covers some activities of credit providers (CPs) using other information, and even the activities of other third parties using information obtained from a CRA or CP. It also clearly defines CRAs so as to regulate their activities 'whether or not the information is provided or intended to be provided for the purposes of assessing applications for credit' (s.6(1)).

I note the quotation at paragraph 2.29 from the Minister's second reading speech on the 1989 amendment Bill which reads in part:

> "The principal purpose of this Bill is to provide privacy protection for individuals in relation to their *consumer credit records*." (our emphasis)

The term 'credit record' is not then used in the Act. However, I submit that the ALRC should recommend that the legitimate wider scope of the regime be recognised by abandoning the narrow term 'Credit reporting' and using instead the more accurate 'Credit information' which should be defined as 'report' is in s.18N(9).

At the same time the implied scope of the terminology could usefully be narrowed – again in line with the second reading speech - by explicit reference to either '*Consumer* or *Personal* credit information' and '*Consumer* or *Personal* credit reporting' (as applicable) to make it clear that the regime is only concerned with information about credit extended to natural persons for a non-business purpose.[2] (Q.5-25)

These two changes would support the intent of the legislation, which the Issues Paper correctly paraphrases in paragraph 2.31 as 'to regulate the collection [etc] of personal credit information.'

While the focus should remain on the use of personal credit information for credit assessment and lending decisions, the review should be mindful of the increasing pressures to use information held

---

[2] I note that the personal v commercial distinction in the credit reporting provisions is different from the distinction in the Privacy Act more generally between natural and legal persons. The definition of personal information as information about natural persons means that information about sole traders and partners that relates to their business affairs is still personal information subject to privacy principles. I make no judgment here about the appropriateness of this wider definition but do not propose any change to the clear distinction between personal and commercial in relation to credit reporting.

by CRAs for other secondary purposes unrelated to credit arrangements' some of which are already expressly allowed under the Privacy Act. A comprehensive review of privacy protection for personal credit information must in particular take account of any use of information held by CRAs for general identity management purposes, either commercially or in relation to government processes.

Another scope issue relates to the definition of 'Credit Provider'. This is addressed under a separate heading below.

Rules cannot be divorced from enforcement

Chapter 4 of the Issues Paper addresses the complaints and enforcement aspects of the Privacy Act in the specific context of the credit reporting provisions. Many of the issues raised here are generic ones already canvassed in Issues Paper 31, and our general answers to Qs 4-1 to 4-4 are contained in our submission on that Paper.

I submit that consideration of the credit reporting provisions must take account of views both on the adequacy of the complaints and enforcement provisions and on the fifteen years experience of how those provisions have been used in practice.

I note that the specific complaint handling requirements in Part 3 of the Code of Conduct in some cases have no equivalent in relation to the NPPs. They include the requirements to refer complaints between CPs and CRAs where relevant (3.3-3.5) and to specifically inform a dissatisfied complainant that they may complain to the Privacy Commissioner (3.7).

The proposal for placing the burden of proof in relation to disputed listings more explicitly on the credit provider (IP 32 paragraph 4.32) has much to commend it – see also our comments on better evidence for defaults below.

In response to Q.4-4, I note that the current inclusion of criminal offence provisions in the Act is not consistent with the general approach to enforcement of information privacy laws through a strict liability civil penalty regime. I suggest that the burden of proof required for successful criminal prosecutions is too high to be a realistic deterrent – I note that there have been no prosecutions to date under Part IIIA. It would seem that civil penalty regimes have proved far more effective for enforcement of financial services and consumer protection laws.

On the specific point of application to acts and practices outside Australia (IP 32 paragraph 5.162 & Q.5-27) I can see no reason why the provisions of s.5B should not apply to Part IIIA. Whatever application the Act has for private sector organisations subject to the NPPs, and the Commissioner's powers, should logically apply also to CRAs and CPs.

Underlying assumptions

The Issues Paper appears to have accepted some of the 'industry' positions as a given. These include a presumption that more credit is a good thing; that risk based pricing is desirable, and that efficiency is a primary goal. I submit that there is a danger that in a detailed discussion of credit reporting regulation may lose sight of a fundamental foundation of privacy law: that individuals are entitled to a presumption of privacy – particularly in the sensitive area of personal finances – with any exceptions needing to be clearly justified on the basis of other public interests that may outweigh the privacy interests of individuals.

It is also desirable to make it clear that this is not just a financial services issue. The actual and potential secondary uses of credit information files and credit reports, and the attraction of them for both legitimate and illegitimate use (e.g. identity management and identity crime) means that the regulation of personal credit information must take into account much wider public interest issues.

In this respect I note the comments made by the Privacy Commissioner in her recent submission on the draft AML-CTF Rules: that these rules leave it unclear as to whether the use of credit history for the purpose of account opening ID verification is authorised by law.[3] I return to this issue below.

Comprehensive reporting

(Qs 6-1 to 6-4)

The Issues Paper chooses to treat the issue of comprehensive reporting[4] as separate from the review of the current regulation (Chapter 6). This is understandable given the history of regulation, and those sceptical of the case for comprehensive reporting are predictably nervous about conceding ground as part of the review of existing rules. However, I submit that the issues cannot sensibly be divorced. Any review of the existing rules inevitably invites questions about each stage of the information life cycle – collection, retention, access, use and disclosure – the answers to which straddle the boundary between negative and positive information.

It is already the case that credit information files are permitted to contain some information that is not necessarily 'negative' such as current credit providers and inquiries, including type and amount of credit sought. The Issues Paper fails to mention this in its introductory history at paragraph 2.23. While the provision for this information is recognised later at paragraphs 3.24 and 4.9-4.10, the Paper does not comment on the important fact that it is not 'negative' information, and erroneously describes the current system as 'negative' in paragraph 6.7. The fact that the existing scheme is already a 'hybrid' strengthens the case for the review to address the issues surrounding comprehensive reporting *at the same time* as the need for changes to Part IIIA and the Code.

'One size fits all' approach undesirable

The current regime includes a presumption that there is only a single level of access to consumer credit information files. I believe this is too simplistic. As a corollary to opening up the issue of what information can be collected and held, there also needs to be a more nuanced debate about different levels of access: who needs access to what information for what purposes? This is picked up in the Issues Paper in the context of inquiry information (paragraph 5.9), and more generally later, but in our view deserves much greater attention as a desirable feature of a reformed regime.

Definitions

Generally, I raise issues relating to definitions as they arise in the context of discussion of information privacy principles below. However, the definition of 'credit provider' is so fundamental to the scope and effect of the regulatory regime for credit reporting, as well as being central to the discussion on permitted uses and disclosures later in this submission, deserves separate and initial consideration. The following paragraphs answer the questions posed in Qs.5-10 to 5-13.

'Credit provider' has the meaning assigned by s.11B, but this includes a discretion for the Privacy Commissioner to extend the meaning in Determinations (as provided for in s.11B(1)(d)(ii)). The Commissioner has significantly extended the meaning in successive Credit Provider Determinations since 1991.

The ALRC asserts that the original policy behind the Commissioner's Classes of Credit Provider Determination, first issued in 1991, was to 'seek to declare as credit providers as wide a range of

---

[3] See http://www.privacy.gov.au/publications/sub-austrac032007.html#Customer

[4] I welcome the ALRC's use of the term 'comprehensive reporting' rather than 'positive reporting' as the latter introduces a bias into discussion. I urge the ALRC to continue to avoid the use of the terms positive or negative reporting – as I point out, the current regime allows more than just 'negative' information.

businesses as practicable and permissible' (IP 32 para 5.84). This express objective is missing from subsequent versions of the Determination (most recently August 2006) but the Commissioner has not been swayed by arguments from consumer and privacy groups that this was a wrong policy aim, and has successively re-made the Determination to similar effect.

I submit that it would be more consistent with the primary privacy protection purpose of the Act, notwithstanding the requirement in s.29 to exercise powers with regard to business efficiency etc, for the Commissioner to expand the definition of credit provider only where, on balance, a strong case can be made for access to information held by credit reporting agencies. If this was the starting point, rather than a declared willingness to expand, then consideration of the compliance issues and proportionality arguments raised during consultations might have led to a more restrictive definition.

I submit that meaning of 'credit provider' should be exhaustively defined in the Act. Inadvertent oversight of legitimate claims (e.g. for mortgage insurance, securitisation arrangements, and assignees) in the original legislation were rectified in early Determinations. These can now be incorporated in a new statutory definition. There has been enough experience of the law to ensure that all legitimate claims for inclusion have been brought to light and accommodated.

The Issues Paper refers in paragraph 5.99 to two specific 'bids' for access to the system from classes of organisation not currently defined as credit providers – mercantile agents (debt collectors), real estate agents and landlords.

There would seem to be no justification for allowing debt collectors direct access as the Act already provides for them to receive information from CIFs and CRs that is relevant to collection of debts via their client Credit Provider. Independent access could therefore only be for more general 'tracing' purposes unconnected to recovery action for a particular debt.

The Parliament expressly excluded the real estate industry from access to the credit reporting system when Part IIIA was originally enacted. Their case was made then and rejected. I am not aware of any new arguments for such access. What has changed since the early 1990s is clear evidence of unsatisfactory tenancy database operation which resulted in four adverse Complaint Determinations by the Privacy Commissioner in 2004[5], and in an agreement by all Australian governments to specifically regulate tenancy databases. These developments strengthen the arguments against access to the credit reporting system for tenancy assessment.

Whatever the definition of credit provider for the purposes of Part IIIA, a related issue is whether it is clear to consumer that they are obtaining credit, with all the implications that flow on from such a transaction. In one complaint, the Privacy Commissioner found that a supplier of medical equipment had failed to make it clear to customers in their documentation that they were entering into a loan agreement,[6] and in another an ambulance service had similarly failed to explain to a 'patient' that he was entering into a credit arrangement.[7]

---

[5] See http://www.privacy.gov.au/act/casenotes/index.html

[6] *R v Medical equipment supplier* [2006] PrivCmrA 17

[7] *C v Service Provider* [2004] PrivCmrA 17

Back to first principles

I submit that a sensible approach to the review of the consumer credit reporting regime under the Privacy Act is to map the current regime, and any proposed changes, onto the 'foundation' National Privacy Principles found in Schedule 3 of the Act. The NPPs, which are the default information privacy standard for all larger private sector businesses, cover the same ground as Part IIIA, the Code of Conduct, and the Credit Reporting Determinations, i.e. collection, data quality, transparency and notice, storage and retention, security, use, disclosure and access and correction. One objective of any reform should be to avoid simple repetition of NPP obligations in the credit reporting 'rules'. Those rules should be confined to additional or more tailored obligations.

I suggest an analytical approach as follows:

Principle	*NPP*	*Additional effect of Pt IIIA, Code & Determinations*	*Desirable changes*	*Options for 'delivery' e.g. supplementary NPP, separate statutory rule, Code rule, Determination, Governance Standard*
Collection				
	(e.g. NPP 1.1)			
	Application to Credit Reporting Agencies (CRAs)			
	Application to Credit Providers (CPs)			
	Application to third parties			

This analysis would be applied firstly to credit reporting agencies, secondly to credit providers, and lastly to third parties.

In Appendix A I have completed the first three columns, for credit reporting agencies. It is beyond our resources to complete the exercise, but our 'desirable changes' (column 3) are outlined in the rest of this submission – but with CRAs and CPs discussed together rather than separately.

The numbers in brackets below refer to the relevant 'cell' in the table at Appendix A.

Collection

Permitted content

(Qs.5-1 & 5-26)

(1) The Act attempts to restrict credit reports to a prescribed set of information, but does so clumsily by prescribing the content of credit information files with both a positive and a negative list (IP32 paragraphs 3.24 & 3.25), and then limiting the content of credit reports to 'permitted categories'.

The application of these limits in practice is complicated by the choice of some CRAs to hold some of the permitted content in separate databases; of identifying particulars on the one hand and of publicly available information including court judgement and bankruptcy orders on the other. Some items within both of these categories of information could be held in a CIF, while others could not, but could be held elsewhere. The other (non-CIF) databases are subject only to the general National Privacy Principles, leading to uncertainty and confusion amongst both data users and data subjects as to their obligations and rights respectively.

In relation to Residential Tenancy data (paragraph 3.58) I note that CPs would be covered by s.18N in respect of any information in an RTD as it is 'has a bearing on … creditworthiness … etc'.

Identifying particulars (2)

In relation to identifying particulars, the Issues Paper explains the current position at paragraphs 3.21-22 but does not discuss the issue further in Chapter 5. I see this as a major omission, as the identifying particulars are critical not only to accuracy of matching – both for commercial access and for 'subject access' by individuals – but also to the value of the CIFs for other uses unrelated to credit assessment.

Inquiry information (3)

In relation to inquiry information, the Issues Paper refers to the submission of the CCLC that this information can be seriously misleading if it is 'assumed' to be negative. While individuals should not be penalised for shopping around for credit, 'comprehensive reporting' (suggested in paragraph 5.8) is not the only solution. Instead, there could be a requirement on CPs not to use inquiry information 'negatively' in their credit assessment processes without first ascertaining from the individual concerned the reason for the inquiries (where this cannot be deduced from a subsequent record of 'current credit provider' status – see below).

Mandatory reporting? (4)

(Q.5-2)

In relation to *current credit provider* information, I note that many CPs do not lodge this information with CRAs, as they are allowed to do under the current regime. I understand this to be partly because the marginal contribution this information can make to credit assessment is outweighed by the commercial value of protecting the identity of their customers. It is also partly because there is a consequential obligation on CPs under s.18F(5) to notify a CRA that an individual is no longer a borrower.

There is also no statutory obligation on credit providers to lodge *default information* with CRAs. CRAs encourage subscribers to provide 'reciprocal' information but cannot insist on them doing so.

This raises the issue of whether reporting – of any or all of the permitted contents - should be mandatory – either as a statutory requirement or as a commercial condition of access to CIFs (IP 32 paragraphs 5.25-5.26).

Any decision to require or allow mandatory reporting would be a major change to the current regime. Financial counselling organisations can see some advantages in mandatory reporting – not least because it would help prevent debt collectors pushing defaulters into taking out new loans rather than re-negotiating existing terms. Mandatory reporting could also be privacy enhancing in that it would potentially make the CIF more 'fit for purpose' (meeting data quality objectives). But it would at the same time reduce privacy by making the content of CIFs less 'consensual'. A separate debate is desirable about the balance to be struck, independently of any debate about comprehensive reporting. I suggest that considerable weight be given to views of financial counselling organisations in relation to this issue, given their practical experience.

Default information (5)

The issue of small debts being listed is canvassed in the Issues Paper (paragraphs 5.11-5.15). I submit that the research conducted by Dun & Bradstreet about the relevance of telecommunications debts is firstly not necessarily applicable to Australia, and secondly not necessarily conclusive as to causality. Even if there was a similar correlation in Australia it does not follow that allowing the use of this information is justified, given the significant consequences for individuals of a 'default' record. I note that the CRA Veda Advantage (was Baycorp) has introduced a voluntary threshold of $100 for telecommunications debts.

I note the discussion of 'unserviceable loans' at paragraphs 5.16-5.17. I submit that this is an important issue for lending policy, but that it is difficult to justify excluding any actual defaults (over a sensible monetary threshold) from 'permitted content' of CIFs given that they are clearly relevant to an individual's capacity to repay other loans. There could however be an obligation on CPs to notify CRAs if any adjudication is made that in relation to a particular default, the transaction was unlawful or unjust. This would at least allow this fact to be taken into account by other prospective lenders. A related issue is whether a default should be removed once the transaction to which it relates has been judged to be unlawful or unfair – see under 'Retention and disposal' below.

Later in the Issues Paper, the ALRC raises the issue of disputed debts (5.134). Clearly a defaulter should not be able to avoid listing indefinitely simply by asserting that there is no debt, but given the substantial evidence of disputed debts being resolved in the borrowers favour, it seems appropriate to have a statutory moratorium on listing while a dispute debt is being resolved within an appropriate court or external dispute resolution (EDR) scheme (see later for discussion about EDR membership). It should be noted that a disputed debt can rapidly escalate due to accrual of charges, fees and interest, as illustrated by a complaint case in which a debt of less than $300 turned into a default listing for more than $1300 less than 18 months later.[8]

Under Part IIIA, defaults listings can only be lodged with a CRA against a guarantor if the guarantor has been notified and if the CP has taken steps to recover the amount owing from the guarantor. Cases handled by the Privacy Commissioner illustrate the various reasons why inappropriate default listings can be made. One reason is failure by CPs to collect and record accurate information about guarantors as distinct from borrowers.[9]

The Commissioner added a further constraint in the Code of Conduct, prohibiting the listing of defaults for any 'statute-barred' debts i.e. those where the CP has failed to take recovery action

---

[8] *G v Credit Provider* [2003] PrivCmrA 5

[9] *S v Telecommunications Provider* [2006] PrivCmrA 18

within the period allowed by the relevant State or Territory legislation (typically six years).[10] Cases periodically arise where CPs have breached this rule.[11] Given its significance, it may be appropriate to locate this obligation in the primary rule rather than leaving it to the Code.

Dishonoured cheques (6)

I note that there is some uncertainty about whether a dishonoured cheque constitutes 'credit', and therefore whether Part IIIA is internally consistent. If it were determined, and widely known, that dishonoured cheques are 'credit', there is the potential for almost any individual or organisation to be a 'credit provider' and gain access to CIFs. This would allow a major expansion of consumer credit reporting well beyond the relatively constrained limits, and beyond the policy objectives of the legislation.

Some statistics on the extent of reporting of dishonoured cheques, and some empirical evidence of the 'problem' would assist the debate.

Court judgements and bankruptcy orders (7)

I note that there is no official definition of 'bankruptcy order' (paragraph 5.18). This is clearly unsatisfactory as it allows too much discretion by CPs and CRAs, and the relationship of this item of permitted content to the Bankruptcy Act should be clarified in the Privacy Act.

Serious credit infringements (8)

There is clearly too much scope at present for different interpretations of the term 'serious credit infringement', especially given the potentially serious adverse consequences for individuals whose CIF includes such a listing. The practice of listing 'missing' borrowers as clearouts (one type of SCI recorded by CRAs) without further investigation[12] should be prohibited, as this is clearly at least potentially misleading.

ID theft flags

It is suggested later in the Issues Paper that CIFs and CRs might be allowed to contain 'warnings' about individuals having been the victim of identity crimes (theft or fraud) (IP 32 paragraph 5.140). This would seem to be both in the interests of consumers, and directly relevant to the primary purpose of credit assessment. It does however require further debate in the context of the wider identity management discussion recommended below.

---

[10] Paragraph 2.8 of the Credit Reporting Code of Conduct

[11] *Q v Credit Provider B* [2005] PrivCmrA 16, and *B v Credit Provider [2005]* PrivCmrA 2

[12] See also IP 32 paras 5.24 and 5.135

Sensitive information

In the context of possible structural reforms, the ALRC raises the possibility of credit information being included in the definition of 'sensitive information' in the Privacy Act. (IP 32 paragraph 7.26) This would have two main consequences – collection would be subject to NPP 10 as well as NPP 1, and secondary disclosures relying on exception 2.1(a) would have to be directly related to the primary purpose of collection (see later). As explained in our submission on IP 31, we are sceptical about the value of NPP 10, which only deals with the permitted circumstances of collection and not with the more significant issues of use and disclosure. In practice, CRAs and CPs would have to satisfy NPP10 by obtaining consent. As I explain below, I believe that any consent for exchanges of information in the credit reporting system is 'spurious' – giving consent is in effect a mandatory condition of obtaining credit. Subjecting CRAs and CPs to NPP10 would be an obstacle to our preferred approach which is to replace consent with a more 'honest' acknowledgement.

Notification

(Qs.5-3 & 5.17)

(11) The notice obligations fall entirely on CPs, on the basis that CRAs have no direct contact with individuals (unless they exercise their rights of access) and therefore have no opportunity to give information to individuals. Leaving aside the important issue of whether these requirements on CPs are honoured and enforced (see IP32 paragraph 5.119), there is a key issue of principle. Given the significance to individuals of a CIF entry, I suggest that there could be an obligation for CRAs to inform individuals periodically of the existence of a CIF entry, and specifically at the time a default listing is made. While these requirements might appear to be onerous, I suggest that the contribution that pro-active notification would make to data quality should more than outweigh the cost.

The law could be clearer about the timing of notice (IP 32 paragraphs 5.27-5.31, and 5.118-5.122). It is unacceptable to allow the requirement to be interpreted to permit notice only at a later stage in the life cycle (e.g. debt assignment or collection) when there is no opportunity for the individual to affect their position. I submit that there should be a requirement to notify at or prior to any significant event including the initial collection (loan application), listing a default, assigning a debt, or commencing debt collection, in addition to the existing requirement to notify refusal of credit on the basis of an adverse credit report.

In the case of default listing, the notice should be required *prior to* listing to give individuals an opportunity to avoid the listing. This would be in the interests of lenders as well. However, the use of the threat of listing to harass individuals, particularly in debt collection (IP 32 paragraph 5.133), must be controlled.

Clearly the notice must be accurate to be effective, and valid under the Act – in a complaint case, the Privacy Commissioner found that a credit provider had notified the borrower of an overdue payment (as required by paragraph 2.7 of the Credit Reporting Code of Conduct) but had incorrectly described it as being only 30 days overdue, instead of the 60 days which was in fact the case and which is the threshold for listing a default.[13] One incidental issue that this case illustrates is the unexplained location of the notice requirement for guarantors in the Act itself (s.18E(1)(ba)(ii)) whereas the equivalent notice requirement for the borrowers themselves has had to be added by the Commissioner in the Code of Conduct.[14] While both requirements have the

---

[13] *A v Credit Provider* [2006] PrivCmrA 1

[14] S.18E(1) requires the credit provider to have taken steps to recover the amount due from both borrowers and guarantors before listing defaults against them, but only in the latter case does the section also expressly require

same effective status, it would be preferable for equivalent requirements to have the same 'location'.

Use & Disclosure

(13) With respect to disclosures by CRAs (Q.5-9), s.18K effectively replaces NPP 2.1, which is a set of permitted purposes, with a more prescriptive set of permitted circumstances, which involve prescription of both purpose and recipient (IP 31 para 5.75).

(14) The first set of permitted disclosures are to credit providers and related bodies, for a range of purposes connected with credit assessment and management. ((1)(a)-(j)). There seems to be general agreement that the purposes covered by these subsections are, in NPP 2 terms, directly related (and within reasonable expectations of someone who understands the way credit industry works – but not of the layman or typical applicant for credit).

The main contentious issue about these 'related purpose' disclosures is the definition of 'credit provider'. This has been discussed above under the 'Definitions' heading.

Consent

(Qs 5-14 and 5.15) (15)

The complex issue of consent and its role in privacy laws has already been canvassed by the ALRC in its general Issues Paper 31, and we have commented on it in our submission on that Paper.

Spurious consent – really only notice

In relation to the operation of the credit reporting regime, I suggest that the requirements for 'agreement' in ss.18K and N to disclosure by CRAs to CPs and by CPs to other CPs could be replaced with requirements for notice. This would acknowledge the reality that all credit providers routinely make 'agreement' to disclose a condition of loan applications. It is not therefore 'free and informed consent' in that individuals cannot in practice proceed with an application for credit without giving their agreement to disclosure. In these circumstances it is more 'honest' and accurate to impose only an obligation to notify – as has already been done for disclosure of information by CPs to CRAs (and effectively for collection by CRAs) by s.18E(8)(c).

The discussion of the NPPs in this context in Issues Paper 32 reflects a particular interpretation on NPP 2.1 with which I do not agree. It is suggested that it may be necessary for Credit Providers to obtain consent for disclosures involved in the credit reporting system because they would not fit within the alternative exception for secondary purposes (paragraphs 5.106-5.107). I submit that it is at least arguable that within the context of the well established operation of the credit market, disclosure to CRAs and other CPs is both a related purpose and within reasonable expectations (NPP 2.1(a). I support the suggestion made elsewhere that CRAs and CPs could do more to educate the general public about credit reporting, thereby strengthening the basis for relying on exception 2.1(a). But I believe a relatively generous interpretation of this exception is in this context preferable to having to rely on consent (2.1(b)) when that consent could not, in the circumstances, be free and informed.

I submit that the Bankers' common law duty of confidentiality, as incorporated in the ABA Code of Banking Practice, should similarly not be used as an excuse for seeking meaningless or spurious 'consent' (IP 32 paragraphs 5-108-5-109). I submit that the disclosure of credit information without

---

notice. It may be thought to be implicit in the recovery action, but if so then why has it been added as a separate obligation for guarantors, and why has the Commissioner felt it necessary to make it express for borrowers?

consent by banks would meet the common law test of being 'in the interests of the bank' as well as, in many cases, being required to meet the bank's duties under legislation.

'Bundled' consent

The issue of 'bundled consent' has also been covered in the more general Issues Paper 31. In the credit reporting context, explored in IP 32 at paragraphs 5.110-5.115, I submit that it is particularly important that consent for secondary purposes such as marketing be clearly separated from any (spurious) consent (or acknowledgement of notice) for the disclosures involved in credit checking and assessment.

I note that guidelines on bundled consent promised by the Privacy Commissioner in early 2005 have yet to be appear, confirming that relying on non-binding guidance is not a sufficient solution to this important issue. What is required is clear statutory prohibition of bundled consent in the context of credit reporting.

Genuine consent for any additional information

Our preference for notice rather than spurious consent outlined above should not be taken as negating the need for *genuine* consent for any exchange of further details as part of any move towards more 'comprehensive reporting'. If one of the characteristics of a comprehensive reporting scheme was a genuinely free choice for consumers as to whether to allow extra details to be listed in a CRA's CIF, then they should of course be offered this choice, but on an express consent or 'opt-in' basis rather than either an implied consent or 'opt-out' basis, or simply being notified that it was a condition of a loan application.

Marketing

(Q.5-16)

(16) The conditional exception for direct marketing available under NPP 2.1(c) is not available to CRAs or CPs under Part IIIA – and it is appropriate that this restriction should remain to re-inforce the clear policy objective of Part IIIA. See above for comments on ensuring that bundled consent cannot be used to bypass this restriction.

One practice that has been identified as possibly breaching the restriction on direct marketing (IP 32 paragraph 5.117) is the use of credit information held by CRAs to 'screen out' those of a CPs existing customers (or new prospects) that do not meet certain criteria – typically using credit scoring or other derived rankings. I understand that CP representatives have suggested in recent discussions with NGOs that using CIF data in this way allow them to avoid making unsolicited offers of credit (either new or increased limits) to consumers who are less likely to be able to service the commitment, thereby contributing to 'responsible lending'. Unfortunately, experience suggests that many CPs use any additional information they can acquire to increase the total volume of offers, inevitably leading to a least some inappropriate offers and to some excessive or unconscionable lending. I understand that some consumer NGOs have argued that access to CIF data be permitted only where the individual has initiated an enquiry or transaction. I submit that such a condition would be consistent with foundation privacy principles.

Disclosure by CRAs and CPs

(Qs.5-9, 5-18 & 5-19 & 5-26)

(20) The exception provided by s.18K(1)(m) is identical to NPP 2.1(g), and could therefore be repealed if a decision was made to strip Part IIIA back to only those requirements that are additional to, or more specific than, those in the NPPs. (see separate discussion later).

(21) The exception provided by s.18K(1)(n) appears to cover similar circumstances as NPP 2.1(f) and (h), but is more tightly limited to disclosures in relation to 'serious credit infringements' which are defined in s.6 as being, in effect, credit related fraud or intended evasion of credit related obligations. This is a very specific type of 'wrongdoing' and leaves CRAs unable to either investigate, or assist enforcement agencies to investigate, any other type of alleged crime or 'wrongdoing', as most organisations can do under the NPP 2. Disclosures can only be made for 'enforcement purposes' under the previous exception where they are expressly required or authorised by or under law (s.18K(1)(m)) e.g. in response to a warrant or subpoena.

(21a) The exception provided by s.18K(1)(k) for information that is publicly available has a similar effect to the exclusion of information in a generally available publication from the application of all the NPPs except the collection principles. However, s,18K(1)(k) creates a loophole that potentially allows CRAs to make the identifying particulars held as part of a credit information file available to third parties for non-credit-related purposes, such as identity verification services, although at least one CRA is uncertain about its ability to provide electronic identification and verification services (IP 32 paragraph 5.139)

These issues are taken up separately by the ALRC in IP 32 paragraphs 5.136-140 and 5.152-160 & Qs 5.22 & 5-23. I suggest that further discussion is required about identity management in general, in the wider context of developments such as the proposed Document Verification Service, the due-diligence requirements of financial services legislation including the *AML-CTF Act 2006* and similar statutory identification obligations such as under the *Telecommunications Act 1997*. It would be sensible for any clarification of the use of credit information files for identification outside the credit reporting context to await the outcome of those wider discussions.

Other conditions of access

(Qs.5-18 to 5-20)

An important potential safeguard in the credit reporting regime which has no direct equivalent in the NPPs is the imposition of standards as a condition of access to the credit reporting system. The Issues Paper mentions suggestions that CPs should only be allowed to participate if they are also subject to the Uniform Consumer Credit Code (UCCC), which contains important consumer safeguards. This would seem to be a sensible protection.

Another condition of access could be membership of a binding and enforceable External Dispute Resolution (EDR) scheme, such as the Banking and Financial Services Ombudsman (BFSO) or the Telecommunications Industry Ombudsman (TIO) (IP 32 paragraph 4.36 & Q.4-3). I understand that while there is a voluntary Credit Ombudsman scheme, not all credit providers – even all those who are subject to the UCCC - are required to be members of a mandatory co-regulatory scheme supported by legislation, and meeting recognised standards.

Making membership of an effective EDR scheme would not only ensure that credit providers accessing the credit reporting system had redress for breaches of non-privacy lending standards, but also that they had access to an alternative and more responsive first instance complaint body for privacy complaints as a first instance alternative to the Privacy Commissioner (see our submission on IP 31 for our views on weaknesses in the Commissioner's complaint handling). Both the TIO and the BFSO have jurisdiction, and agreements with the Privacy Commissioner, to handle complaints about breaches of the NPPs in the first instance, and these arrangements could be extended to breaches of the credit reporting provisions of the Privacy Act.

I note in this context that telecommunications providers (telcos) are subject to a mandatory Credit Management Code[15] which, amongst other things, limits the circumstances in which a telco can list a default against a customer with a CRA. Any amendment of the credit reporting provisions of the Privacy Act should acknowledge and provide for mandatory 'higher' standards in or under other specific legislation.

Automated decision-making

Another condition of use which has a precedent in data protection laws in the European Union is a prohibition on wholly automated decision-making, specifically in the context of credit assessment.[16] There is also a precedent in Australian law for a 'no-automated decision' condition – that is in the *Data-matching Program (Assistance & Tax) Act 1990*, section 11 of which requires notice to individuals before any adverse action can be taken based on the results of data matching between specified Commonwealth agencies. This gives the individual the opportunity to challenge the information and to have a human review of any proposed action.

I understand that fully automated assessment of loan applications is common, using highly sophisticated credit scoring systems. However predictive and accurate these systems are, and however efficient they are compared to human judgement, they cannot be 'fair' in all individual cases. The requirement to notify loan applicants of adverse credit reports, and of their right of access to their CIF (s.18M), only goes some way towards ensuring fairness. Credit providers could be required to offer applicants an opportunity for a human review of any adverse decision.

Data quality

(Qs 5-5 and 5-8) (24)

Both s.18G(a) and s.18J(1) imposes an obligation on both CRAs and CPs to take reasonable steps to ensure that personal information in a CIF or CR (narrower definition) is 'accurate, up-to-date, complete and not misleading'. S.18J(1) differs from s.18G(a) only in specifying that 'reasonable steps' include making 'appropriate corrections, deletions and additions'. While the rest of s.18J is concerned with changes requested by an 'individual concerned', the obligation in 18J(1) is independent of any such request and therefore applies however a CRA or CP becomes aware of data quality problems.

The obligation s.18G(a) and s.18J(1) is the same obligation as applies to all organisations subject to NPP 3, with the addition of the 'not misleading' criterion. Ideally, it would be desirable to make the data quality obligation consistent. As we suggested in our submission on IP31, this could be achieved by amending NPP 3 to add 'not misleading'. The alternative of deleting 18G(a) and defaulting to NPP 3 would be a retrograde step - given a broad consensus that CIFs held by CRAs have some major data quality deficiencies (paragraphs 5.43-5.53), all quality criteria should be maintained.

The obligation imposed by the Code of Conduct on CRAs to investigate suspicions of inaccuracy, and to report to the Privacy Commissioner (described in paragraph 5.42), should also be maintained, although it is not clear how frequently these obligations are being invoked. Greater transparency would aid an assessment of the value of these requirements.

One source of poor data quality is failure to adequately record separate details for borrowers and guarantors. In one case conciliated by the Privacy Commissioner, a default listing was placed on a

---

[15] Australian Communications Industry Forum (now Communications Alliance) Code C541, 2006

[16] Directive 95/46/EC Article 15 - see http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

guarantor's CIF because the credit provider had failed to separately collect and record an address for the guarantor as distinct from the borrower.[17]

I agree with the CCLC analysis that there are too few incentives, and too few sanctions to ensure compliance with the data quality obligations. While the main CRA has taken helpful voluntary steps to improve data quality, I submit that the following additional obligations are desirable:

- CRAs to include data quality obligations in subscriber agreements; monitor and conduct regular checks on quality, and investigate any possible breaches (as in the New Zealand Credit Reporting Privacy Code – see paragraph 5.55)
- CPs to provide CRAs with evidence to support listings (requirements noted by the 2005 Senate Committee)

I also refer to my earlier suggestion that a requirement for routine communication between CRAs and all individuals who are the subject of a CIF would result in a major improvement in data quality, to the benefit of both consumers and lenders.

As the ALRC acknowledges, the current system is an 'honour system' (IP 32 paragraph 5.53). One potential measure that has been suggested is a requirement on CPs to provide evidence to CRAs of a default before the CRA would list it (IP 32 paragraph 5.56), but the industry contends that this would be far too onerous and costly. I suggest that at the very least, there should be a statutory obligation on CPs to provide evidence to support a default listing, on request from either a CRA or the Privacy Commissioner (or other relevant EDR scheme), and of course on request from the individual concerned – although this may already be required by other laws.

Multiple listings

There have been many instances of multiple listing, including in cases handled as complaints by the Privacy Commissioner, although none of these have led to formal Determinations (see our submission on IP 31 for criticism of the Commissioner's unwillingness to make Determinations). They include instances of straightforward duplication[18], and unlawful listing of the same default by an assignee[19].

It is essential in the interests both of borrowers and of lenders that ways be found to reduce the incidence of multiple listings (this is addressed in paragraphs 5.36-5.39, but I see this as more a data quality issue than as about deletion). I suggest that a clear distinction could be made between marginal changes in the amount owing on a single debt (often as a result of fees and charges) and a second default on the same loan (or an SCI), separated by a period of 'normal' repayments. It is legitimate for such second defaults (or SCIs) to be listed separately whereas it is in no-one's interests for a single default to be reported and recorded multiple times. However, default on a scheme of arrangement should be not be treated as a separate event so as to trigger a new five year listing. The discussions that are taking place about listing of schemes of arrangement, including the possibility of a shorter retention period are welcome. (paragraphs 5.38-5.39).

If a case can be made for needing an accurate record of the amount of a default, then the law could provide for updating of overdue payment records as a clear alternative to a new separate listing (paragraph 5.37).

To improve data quality, there could be *both* a requirement for assignees to take reasonable steps to check whether the original credit provider has already listed an overdue payment *and* an obligation

---

[17] *S v Telecommunications Provider* [2006] PrivCmr 18
[18] *W v Credit Provider* [2006] PrivCmrA 22
[19] *Q v Credit Provider B* [2005] PrivCmrA 16

on CPs assigning debt to inform the assignee which if any of the assigned debts have been reported to one or more CRAs (and if so which ones).

All these suggested new requirements (and some existing ones) might be facilitated by a system of identifiers for loans (as opposed to borrowers). This should be explored with the finance industry.

Security

Security measures

(Q.5-6) (25)

The security obligation on CRAs and CPs under s.18G(b) is similar to the general obligation in NPP 4.1, but with the addition of another type of risk – that of unauthorised use (as well as unauthorised access, modification and disclosure).

Section 18G(c) adds an additional obligation based on that in IPP 4 (applying to Commonwealth agencies) to take steps to ensure security when giving personal information to a third party service provider

Retention and disposal

(Q.5-4) (26)

In contrast to the general 'dispose when no longer needed' obligation of NPP 4.2, Part IIIA currently sets three specific retention periods – 5 years for overdue payment (default) and other 'negative' information, and inquiry information; 7 years for bankruptcy and serous credit infringement (SCI) information, and 14 days for current credit provider status information after notice from a CP that it is no longer a current credit provider.

I suggest that a finer-grained regime, with differential collection and access rules, such as I suggest elsewhere in this submission, needs to be accompanied by a more graduated set of retention periods for different types of information and circumstances.

Simply defaulting to the general NPP 4.2 obligation would leave CRAs and CPs with too much discretion – this is an area in which more rather than less prescription is desirable.

For consistency, the statute-barred override that currently applies to guarantors should also apply to other individuals' CIFs and in both cases should be subject to an 'anti-abuse' condition that default information cannot be listed more than a year after the issue of a default notice (paragraphs 5.33-5.35).

CPs are required to notify CRAs when a previously listed default has been repaid, such that there is no longer an overdue payment (s.18F(3)). However, the CRA is only required to add a note to that effect, not remove the listing, which can stay on the CIF for up to five years (see below). The potential effect of this long-term negative information lies at the heart of much NGO dissatisfaction with the current system. I suggest that a revised regime could provide for, and in some cases mandate, earlier removal of default listings for smaller debts and in a range of other 'mitigating' circumstances.

I also support the suggestion referred to above that a default listing should be removed once the transaction to which it relates has been judged to be unlawful or unfair.

Access and Correction

(Q.5-8)

(29 & 30) Part IIIA provides for access by individuals to information about themselves held by CRAs in CIFs and by CRAs and CPs in CRs (s.18H) but this is not as detailed as NPP 6 which also applies. NPP 6 also applies to *other* personal information held by CRAs and CPs, including information held by CPs covered by the wider definition of 'credit report' in s.18N(9). This other information will include credit scores and other 'rankings' derived from analysis of credit information. Australian CRAs and CPs rely on the 'evaluative information' exception in NPP 6.2 to avoid giving individuals actual credit scores or rankings – providing them instead with an 'explanation'. In contrast, the NZ Credit Reporting Privacy Code does require a Credit Reporter (equivalent to a CRA in Australia) to give access to all credit information (Rule 6) including credit scores (Commentary on Rule 6)[20]

I suggest that there should be a clear statutory right of access to credit scores and other rankings held by CRAs and CPs, together with explanatory material on scoring systems and current thresholds for acceptance, to allow individuals to better understand how they are being assessed.

I acknowledge that different scoring systems are used both within and between organisations, that scores will vary over time with the same information and may only be held temporarily, and that while CRAs provide scoring services to some clients, will not necessarily hold a score for every individual with a CIF. I also acknowledge that scoring systems are highly valued and closely guarded commercial assets. However, given the significance of scores for individuals, none of these factors are sufficient reason why individuals should not be allowed to see their scores. The fact that the largest Australian CRA has been able to operate under the NZ Code suggests that this requirement is not too onerous.

Charges for access (32)

All three Australian CRAs currently offer a form of access free of charge, but this is at their discretion. Given the significant impact of credit information files to individuals, and the value to the overall system of individuals checking their records, I suggest that a strong case can be made for access to CIFs and CRs to be free of charge as of right, rather than just that any charge be 'not excessive' (NPP 6.4)

Annotation as an alternative (34)

NGOs have submitted that s.18J does not expressly require correction rather than mere annotation (IP 32 para 5.72). This is a debatable interpretation of the quality requirements in 18G(a) and 18J(1) but for the avoidance of doubt, the law could be amended to require correction where it is objectively determined that information is inaccurate, out of date, incomplete or misleading.

[20] It would seem that the conditional Trade Secrets exception in s.28 of the Privacy Act 1993 (NZ), while apparently similar to the NPP 6.2 grounds, do not allow NZ Credit Reporters to withhold credit scores.

Interaction of Rules and Principles

As with all sets of information privacy principles, it is often difficult to isolate the effect of any particular rule or principle in credit reporting. Complaints about breaches of credit reporting provisions typically include issues of data quality, security, use and disclosure and collection, and also involve actions both by a CRA and one or more CPs.

Returning to the questions asked in the Chapter on the Regulatory Framework (Qs 4-1-4-4), many abuses of access to credit information, even when detected and reported, fall foul of the division of responsibility between CP and CRA, and of the Privacy Commissioner's typically narrow investigation of complaints, often choosing to focus on the superficial grounds visible to the complainant rather than following leads into other potential breaches both by the immediate respondent and the other party (CP or CRA).

If a credit provider with legitimate access to a CRA wishes to deliberately abuse its position to obtain information about individuals who are not borrowers, it is open to it to do so in a number of ways. One was highlighted in a complaint case in which a CP had required a potential employee to complete a loan application form, giving consent to a credit reference check, when in fact no loan was involved.[21] This case was referred to the Federal Police for investigation of possible Part IIIA offences, but due to insufficient evidence was returned to the Privacy Commissioner for adjudication of breaches of other provisions, and ultimately conciliated with compensation paid.

This case usefully illustrates how ineffective the credit reporting provisions are in a number of respects. The obvious questions about both the data quality and security practices of the CRA in accepting an inquiry listing without any evidence were not explored by the Commissioner. The difficulty of proving an offence, to the standard required for criminal prosecution was demonstrated. And the respondent, despite being found to have engaged in deliberately deceptive conduct, escaped with a trivial financial penalty, and, as far as the public knows, with continued access to credit information.

This brings me back to the suggestion made earlier that any re-design of the credit reporting provisions needs to have regard not just to the superficial attraction and meaning of any particular rule, but also to the way in which complaints about breaches of that rule could play out in practice, in light of the now considerable experience. I suggest that any proposed changes need to be road-tested by applying the circumstances of past complaints, to see what effect the changes would have on the ease of investigation, allocation of responsibility, and outcome.

[21] *H v Credit Provider*[2004] PrivCmrA18

The approach to reform

(Q.7-1)

Chapter 7 of the Issues Paper canvasses several options for structural reform of credit reporting regulation.

Views on structural reform will clearly be coloured by judgements about how well the current regime has worked, and there are clearly very different perspectives.

In considering moving some of the 'rules' into more easily changed instruments such as Regulations and Codes, the benefits of flexibility have to be balanced against the risk of changes contrary to the interests of consumers.

In recent years, some CRAs and CPs have shown a greater willingness to acknowledge compliance problems and to engage with consumer organisations, many of whom experience at first hand the harm caused to consumers by reckless lending (often not even using the information currently available) and by systemic practices which contribute to poor data quality.

However there is no guarantee that allowing more flexibility would not result, over time, in less protection for individuals. I believe it is consistent with the policy objectives of the Credit Reporting provisions to retain some prescriptive statutory rules for the collection, use and disclosure of credit information. These need not remain in a separate Part IIIA, but could instead be expressed as additional NPPs applying only to CRAs and/or CPs as appropriate.

Amendments to these rules should be considered on their merits, and where existing rules only duplicate obligations under the NPPs, they can be repealed, provided that all users of the credit reporting system are brought under the NPP regime, by removing them from the small business exemption. This could be easily achieved by amending s.6D(4) to expressly include 'participating in a credit reporting system'.

I suggest that it should be possible to simplify the overall regulatory framework by consolidating the current mix of Part IIIA, Determinations and Code. As suggested above I favour incorporating the substance of the existing Privacy Commissioner Determinations into the Act – there is now sufficient experience of the expanded definitions of 'credit provider' and of permitted CIF contents for a consensus position to be included in the Act. Codifying these definitions in the legislation would provide valuable protection against further 'function creep'.

In contrast, some of the detailed provisions in Part IIIA could be moved into a Code. Again, each proposed change or relocation should be considered on its merits. If the Act is changed, as has been suggested in response to IP 31, to allow the Commissioner to *initiate* and make binding Codes under Part IIIAA, then the Credit Reporting Code of Conduct could be re-made under this Part.

I understand that one of the major Australian CRAs has proposed the introduction of Data Governance Standards (DGS) as a complementary layer of regulation. DGS would be developed and proposed by individual organisations to set out the processes by which they would comply with the statutory or Code rules. The DGS would however, once registered, become binding on the organisation under the Act, and a breach of the DGS would be treated as an 'interference with privacy' for the purposes of the complaint and enforcement provisions, in the same way as a breach of the NPPs, or Part IIIA or a Code would be.

I cautiously welcome the concept of DGS, although I suggest a different terminology – 'standard' implies a substantive compliance criteria rather than a process matter such as I understand the proposed DGS would address. I would see a Data Governance 'plan' as explaining how a particular organisation intends to comply with the 'standards' set in the Act or Code.

I would not however see a DGS (or DGP) as an alternative to the required standards being set out elsewhere. Given that there would possibly be multiple DGS/DGP addressing the same compliance issues, but in organisation-specific ways, they could not set a substantively different standard – otherwise individuals would have different levels of enforceable rights depending on who they dealt with.

The suggestion that the regulation of credit reporting be moved out of the Privacy Act (IP32 paragraph 7.28) has some attractions – mainly the better 'fit' with regulation of financial services and the UCCC, and the prospect of enforcement by a more pro-active regulator with greater powers, such as ASIC. However the substance of credit reporting regulation is clearly fair information handling, which places it squarely in the area of data protection or information privacy law.

On balance, I suggest that the regulation of credit reporting should remain within the Privacy Act, with any shortcomings of that Act and its enforcement being addressed without delay. The wider ALRC Review will hopefully result in significant improvements, such that the Privacy Act can be an effective 'home' for credit reporting regulation.

Appendix A: Comparison of Credit information rules with NPPs

(incomplete draft - suggested as an analytical tool)

A. Credit Reporting Agencies (CRAs)

Principle	**NPP**	**Additional effect of Pt IIIA, Code & Determinations**	**Analysis and Desirable changes**	**Options for 'delivery' e.g. supplementary NPP, separate statutory rule, Code rule, Determination, Governance Standard**
			Numbers are references to paragraphs in the submission	*See submission – not yet 'itemised'*
Collection				
	NPP 1.1 - necessary	No discretion – permitted content is specified in s18E and Determ 1991 No 2	(1)	
		Identifying particulars (Determ 1991 No 2)	(2)	
		Inquiry information (18E(1)(b) (i),(ia),(ii),(iii),(iv))	(3)	
		Current credit providers (18E(1)(b)(v))	(4)	
		Default (18E(1)(b)(vi))	(5)	

Principle	**NPP**	**Additional effect of Pt IIIA, Code & Determinations**	**Analysis and Desirable changes**	**Options for 'delivery' e.g. supplementary NPP, separate statutory rule, Code rule, Determination, Governance Standard**
			Numbers are references to paragraphs in the submission	*See submission – not yet 'itemised'*
		Dishonoured cheques (18E(1)(b)(vii))	(6)	
		Court judgments or bankruptcy orders (18E(1)(b)(viii),(ix))	(7)	
		Serious credit infringement (18E(1)(b)(x))	(8)	
		Overdue payment by guarantor (18E(1)(ba))	(5)	
		A note initiated by the individual (18E(1)(c) & (d))	(9)	
		A record of a disclosure as required by s18K(5) (18E(1)(d))	(10)	
	NPP 1.2 – lawful and fair means	No extra rules		

Principle	**NPP**	**Additional effect of Pt IIIA, Code & Determinations**	**Analysis and Desirable changes**	**Options for 'delivery' e.g. supplementary NPP, separate statutory rule, Code rule, Determination, Governance Standard**
			Numbers are references to paragraphs in the submission	*See submission – not yet 'itemised'*
	NPP 1.3 & 1.5 – making individuals aware	Indirect requirements arising from obligation on CP not to lodge information with a CRA without having first informed the individual (s.18E(8)(c))	(11)	
	NPP 1.4 Direct collection where possible	No extra rules	(12)	
Use & Disclosure	NPP 2.1 & 2.3 – Use and disclosure limits	Use – no extra rules on *use* by CRAs Disclosure by CRA regulated by s.18K – specific exceptions follow:	(13)	
	2.1(a) – related use within expectations	No such discretion – limits override NPP	(14)	

Principle	**NPP**	**Additional effect of Pt IIIA, Code & Determinations**	**Analysis and Desirable changes**	**Options for 'delivery' e.g. supplementary NPP, separate statutory rule, Code rule, Determination, Governance Standard**
			Numbers are references to paragraphs in the submission	*See submission – not yet 'itemised'*
	2.1(b) – express or implied consent	Various provisions in ss.18K & 18N requiring 'agreement' by individuals for certain disclosures of information in a credit report (note wider meaning of credit report under s.18N)	(15)	
	2.1(c) – direct marketing	Not permitted – limits override NPP	(16)	
	2.1(d) – health info for research or stats	N/A – no health info held	(17)	
	2.1(e) – serious/imminent threat	No provision for disclosure	(18)	
	2.1(f) – investigating unlawful activity	18K(1)(n) not as constrained as NPP 2.1 (f) or (h) but limited to SCI – No provision for disclosure for other investigations	(19)	

Principle	**NPP**	**Additional effect of Pt IIIA, Code & Determinations**	**Analysis and Desirable changes**	**Options for 'delivery' e.g. supplementary NPP, separate statutory rule, Code rule, Determination, Governance Standard**
			Numbers are references to paragraphs in the submission	*See submission – not yet 'itemised'*
	2.1(g) -required or authorised by or under law	18K(1)(m) = NPP 2.1(g)		
	2.1(h) – assisting enforcement bodies	18K(1)(n) not as constrained as NPP 2.1 (f) or (h) but limited to SCI - No provision for disclosure for other investigations		
		18K(1)(k) – publicly available information		
	NPP 2.2 – records where using or disclosing for enforcement	Nothing in Part IIIA, but NPP 2 could apply?	(22)	

Principle	**NPP**	**Additional effect of Pt IIIA, Code & Determinations**	**Analysis and Desirable changes**	**Options for 'delivery' e.g. supplementary NPP, separate statutory rule, Code rule, Determination, Governance Standard**
			Numbers are references to paragraphs in the submission	*See submission – not yet 'itemised'*
	NPP 2.4-2.6 – using and disclosing for health services	N/A – medical history or physical handicaps not allowed in CIFs or CR ? any health related information that could creep in – if so NPP 10 may apply	(23)	
Data quality	NPP 3 – data quality measures	s.18G(a) has additional criterion 'not misleading' 18J(1) obligation to correct etc not tied to request from individual	(24)	

Principle	**NPP**	**Additional effect of Pt IIIA, Code & Determinations**	**Analysis and Desirable changes**	**Options for 'delivery' e.g. supplementary NPP, separate statutory rule, Code rule, Determination, Governance Standard**
			Numbers are references to paragraphs in the submission	*See submission – not yet 'itemised'*
Data Security	NPP 4.1 – security measures	s.18G (b) equivalent to NPP 4.1 with additional risk of 'unauthorised use' s.18G (c) has no direct equivalent in NPP 4 (arguably implicit in 4.1) but is identical to the IPP 4 obligation on Commonwealth agencies – limited to risks of unauthorised use and disclosure	(25)	
	NPP 4.2 – retention and disposal	s.18F sets specific retention periods for particular types of information in CIFs	(26)	
Openness	NPP 5.1 – privacy policy	Nothing in Part IIIA	(27)	
	NPP 5.2 – answer queries	Nothing in Part IIIA	(28)	

Principle	**NPP**	**Additional effect of Pt IIIA, Code & Determinations**	**Analysis and Desirable changes**	**Options for 'delivery' e.g. supplementary NPP, separate statutory rule, Code rule, Determination, Governance Standard**
			Numbers are references to paragraphs in the submission	*See submission – not yet 'itemised'*
Access & Correction	NPP 6.1 - access	s.18H obligation on CRAs to give access to CIF and CR (but not wider CI which is subject only to NPP 6.1)	(29)	
	NPP 6.2 – explanation alternative	Nothing in Part IIIA but 6.2 of direct relevance to wider CI info such as credit scores	(30)	
	NPP 6.3 – use of intermediary	Nothing in Part IIIA	(31)	
	NPP 6.4 - charges	Part IIIA silent on charges	(32)	
	NPP 6.5 - correction	18H data quality obligation has additional grounds of 'not misleading' and implicitly includes 'on request from individual'	(33)	

Principle	**NPP**	**Additional effect of Pt IIIA, Code & Determinations**	**Analysis and Desirable changes**	**Options for 'delivery' e.g. supplementary NPP, separate statutory rule, Code rule, Determination, Governance Standard**
			Numbers are references to paragraphs in the submission	*See submission – not yet 'itemised'*
	NPP 6.6 annotation alternative	s.18J(2) specifically requires annotation on request s.18J(3) provides for PC adjudication on length of statement	(34)	
	NPP 6.7 – reasons for denial	Nothing in Part IIIA	(35)	
Identifiers	NPP 7.1 – adopting Cwth nos	Nothing in Part IIIA	(36)	
	NPP 7.2 – use or disclosure of Cwth nos	Nothing in Part IIIA PC Determination allows storage and use of State & Territory Drivers Licence numbers in CIF	(37)	
Anonymity	NPP 8 – where lawful and practicable	No specific rules	(38) Limited applicability – NPP suffices to allow anonymous enquiries about general policies	N/A

Principle	**NPP**	**Additional effect of Pt IIIA, Code & Determinations**	**Analysis and Desirable changes**	**Options for 'delivery' e.g. supplementary NPP, separate statutory rule, Code rule, Determination, Governance Standard**
			Numbers are references to paragraphs in the submission	*See submission – not yet 'itemised'*
Transborder data flows	NPP 9 - conditions	Nothing in Part IIIA	(39)	
Sensitive Information	NPP 10	None of the s.6 'sensitive' information is expressly allowed in CFIs or CRs, but Type of credit may in some cases infer something about health status? Court judgements could include criminal record?	(40)	

B. Credit Providers (CPs)

Principle	**NPP**	**Additional effect of Pt IIIA, Code & Determinations**	**Desirable changes**	**Options for 'delivery' e.g. supplementary NPP, separate statutory rule, Code rule, Determination, Governance Standard**
			Numbers are references to paragraphs in the submission (incomplete)	*See submission – not yet 'itemised'*
Collection	NPP 1.1 - necessary			
	NPP 1.2 – lawful and fair means	No extra rules		
	NPP 1.3 & 1.5 – making individuals aware	Specific requirements in 18E(8)(c) for CP to inform the individual that the information might be disclosed to a CRA at the time of or before acquiring [that] information. More specific about content (than NPP 1.3(d))and timing of notice.	(11)	
	NPP 1.4 Direct collection where possible	No extra rules		

Use & Disclosure	NPP 2.1 & 2.3 – Use and disclosure limits	**Use of CR** by CPs regulated by s.18L – only for assessing application for credit, but specific exceptions:	(3) - Needs rules about fair credit assessment processes	
		Assessing risks in securitisation arrangements 18L(1)(aa)&(ab)		
		Assessing commercial credit applic by the individual (a)		
		Assessing guarantor (b)		
		Internal management (ba)		
		Assisting individual to avoid default (c)		
		Collection of overdue payments (d)&(e)		
		In connection with a serious credit infringement (f)		
		Must not use without (first?) deleting any information not permitted to be in a CIF under s.18E(1)	Unclear what this adds – CRA would be in breach of s18E(1) if any info included that was not permitted. Also ambiguous as to timing of deletion – does requirement imply a universal cleaning or is it OK to identify and delete only at point of use?	

		Use of info about commercial credit or creditworthiness (not otherwise regulated by Part IIIA) only with specific consent, normally in writing (18L(4)&(4A) – can be further prescription in a Commissioner's Determination (18L(6)-(8)) but none yet made?		
		Disclosure of CR or other creditworthiness info by CPs regulated by s.18N – specific exceptions follow. Unlike NPP 2 they are expressed in terms of organisations rather than purposes:		
	Only if for one of the following exceptions apply	Only if permitted content for a CIF (see s18(E)(1) and one of the following applies		
	2.1(a) – related use within expectations	No such discretion – limits override NPP		
	2.1(b) - express or implied consent	S18N(1)(ga) specifically allows disclosure to the individual or another person authorised by them		

	2.1(c) – direct marketing			
	2.1(d) – health info ore research or stats			
	2.1(e) – serious/imminent threat			
	2.1(f) – investigating unlawful activity	18N(1)(h) not as constrained		
	2.1(g) -required or authorised by or under law	18N(1)(g) = NPP 2.1(g)		
	2.1(h) – assisting enforcement bodies	18N(1)(h) not as constrained		
	NPP 2.2 – records where using or disclosing for enforcement	Nothing in Part IIIA, but NPP 2 could apply?	(22)	

	NPP 2.4-2.6 – using and disclosing for health services	N/A – medical history or physical handicaps not allowed in CIFs or CR ? any health related information that could creep in – if so NPP 10 may apply		
Data quality	NPP 3 – data quality measures	s.18G(a) repeats NPP 3 but has additional criterion 'not misleading' 18E(8) prevents CP from disclosing to a CRA unless reasonable grounds for believing info is correct	(24)	
Data Security	NPP 4.1 – security measures	s.18G (b) equivalent to NPP 4.1 with additional risk of 'unauthorised use' s.18G (c) has no direct equivalent in NPP 4 (arguably implicit in 4.1) but is identical to the IPP 4 obligation on Commonwealth agencies – limited to risks of unauthorised use and disclosure	(25)	

	NPP 4.2 – retention and disposal	Nothing in Part IIIA ??		
Openness	NPP 5.1 – privacy policy	Nothing in Part IIIA		
	NPP 5.2 – answer queries	Nothing in Part IIIA		
	No NPP equivalent	Specific requirement on CP to give individual written notice if credit refused wholly or partly on information derived from a CR (s18M) – details vary depending on whether info is about the applicant, a joint applicant or a guarantor		
Access & Correction	NPP 6.1 - access	s.18H obligation on CPs to give access to CR (but not wider CI which is subject only to NPP 6.1)	(29)	
	NPP 6.2 – explanation alternative	Nothing in Part IIIA but 6.2 of direct relevance to wider CI info such as credit scores	(30)	
	NPP 6.3 – use of intermediary	Nothing in Part IIIA	(31)	
	NPP 6.4 - charges	Part IIIA silent on charges	(32)	

	NPP 6.5 - correction	18H data quality obligation has additional grounds of 'not misleading' and implicitly includes 'on request from individual'	(33)	
	NPP 6.6 annotation alternative	s.18J(2) specifically requires annotation on request s.18J(3) provides for PC adjudication on length of statement	(34)	
	NPP 6.7 – reasons for denial	Nothing in Part IIIA	(35)	
Identifiers	NPP 7.1 – adopting Cwth nos	Nothing in Part IIIA		
	NPP 7.2 – use or disclosure of Cwth nos	Nothing in Part IIIA PC Determination allows storage and use of State & Territory Drivers Licence numbers in CIF, and therefore by CPs as an identifier		
Anonymity	NPP 8 – where lawful and practicable	No specific rules	Limited applicability – NPP should suffice to allow anonymous enquiries about general policies	N/A

Transborder data flows	NPP 9 - conditions	Nothing in Part IIIA		
Sensitive Information	NPP 10	None of the s.6 'sensitive' information is expressly allowed in CFIs or CRs, but Type of credit may in some cases infer something about health status? Court judgements could include criminal record?		

C – Repeat for other Organisations accessing CRA CIFs