

Review of Australian Privacy Law

Discussion Paper

Submission to the ALRC

December 2007



Introduction

ANZ welcomes the opportunity to provide further comment to the Australian Law Reform Commission's Review of Privacy.

The ALRC's discussion paper details a large number of specific reform proposals for public comment. ANZ does not propose to respond to each proposal, rather this submission responds to those elements of the discussion paper which are of particular importance to our operations. ANZ participated in the preparation of both the Australian Bankers' Association (ABA) and Australian Retail Credit Council (ARCA) submissions to the ALRC and broadly supports their recommendations.

ANZ believes that given the complex nature of many of the reform proposals and the potential impact they will have on many organisations, that there should be further opportunity for industry to be consulted on key proposals. Consultations could take place once the proposals have been considered by Government.

Response

Developing Technology

The ALRC makes a number of recommendations intended to accommodate developing technology in a regulatory framework. The ALRC proposes that the Privacy Act should be 'technologically neutral' (ie. not refer to any specific technology) in order to ensure that the Act remains flexible and relevant in the case of technological change. While ANZ supports the Act being 'technologically neutral', the discussion below addresses some specific concerns.

Standards

The ALRC recommends that the Privacy Act should be amended to empower the Minister responsible for the Privacy Act (currently the Attorney General), in consultation with the Office of the Privacy Commissioner, to determine which privacy and security standards for relevant technologies should be mandated by legislative instrument. (proposal 7-2)

ANZ is of the view that the existing standards framework provides adequate incentives for organisations to ensure that their technology, both hardware and software, adequately meets privacy and security standards. Given the rapidly evolving nature of information technology, ANZ does not believe that privacy and security standards for relevant technology should be legislated and that for this reason organisations should have flexibility as to the kinds of standards they employ. Technology can quickly become redundant and legislation establishing specific privacy and security standards for relevant technologies could quickly become outdated and would require frequent review.

Automated decisioning/Human review

The ALRC expresses a view that computer software and hardware does not necessarily produce accurate and reliable results in automated decision models, and proposes (in the interests of both organisations and their customers) that the Privacy Commissioner should issue guidance on when a human review of automated decisions is necessary. (proposal 7-5)

ANZ has considerable experience in the use of automated decisioning models. In ANZ's experience, well designed models do not produce inaccurate or unreliable results and have not generated consumer dissatisfaction. Automated decisioning tools are used by ANZ to assess applications for credit cards, credit limit increases and personal loans. ANZ's credit scoring models have been developed using more than 150 variables that predict credit performance. Some of the variables these models employ include: the number of times a customer has exceeded their credit limit; length of banking/lending relationships with ANZ; monthly income against monthly expenditure; and the performance of the customer on other credit products held with ANZ.

Credit scoring is widely recognised as the industry standard for credit assessment and is considered to be more accurate and present lower risks than manual procedures which are more susceptible to risk of human error and bias. ANZ's own analysis supports the view that credit scoring is a consistently more reliable assessment method than manual assessment of a customer's financial information, for the reason that manual assessment is reliant on the accuracy and currency of information provided by individuals. ANZ approves around 50 per cent of the total number of credit card applications it receives. ANZ also conducts manual assessments of all credit card applications which are deemed to be borderline (approximately 20 per cent of all applications) and approves approximately 50 per cent of these applications following the manual assessment process.

ANZ believes that different assessment methods are more appropriate at different stages of the customer's relationship with a credit provider. Manual assessment of financial information is the most appropriate method to properly assess new applicants for credit where there is a lack of any other information. ANZ does not generally rely on the score of a customer to assess capacity for a credit card limit increase offer until that score can be based on 9 months of the customer's transactional and repayment data. Where ANZ has built up information about a customer's credit behaviour over this timeframe, automatic scoring is a more reliable technique to assess credit applications.

ANZ conducted a study in 2005 into the credit behaviour of a group of recently acquired credit card customers who were approved through assessment of their self-reported financial details with a group of existing customers who had accepted a credit limit increase offer and were assessed using ANZ's credit scoring methods. Over a six month period, 1.7 per cent of the first group of customers showed signs of financial stress (for this study, financial stress was defined as being 30 days late on a payment on one or more occasions.) During the same period, only 0.6 per cent of those assessed by behaviour scoring displayed signs of financial stress.

ANZ conducted a further analysis of the ANZ customer base in the ACT to assess the reliability of credit assessment based on financial information provided by a sample of customers. The results of this study suggested that legislation in the ACT which requires that all credit limit increase applications be assessed through manual assessment methods has not reduced the rate of defaults. The research also provided some insight into the reliability of credit assessments based on financial information provided by customers. For example, the study found that 24 per cent of credit applications could not be processed due to errors and omissions of financial details. Around half of these applications contained obvious data errors while the other half appeared to contain incorrect income details when viewed in conjunction with the living expenses stated.

Although the ACT legislation prescribes only one form of assessment, ANZ has chosen to continue to apply credit scoring assessment methods to these customers in addition to the required manual assessment. This decision is based on credit risk considerations and a reliance on credit scoring as the most reliable and robust technique for assessing existing customers.

Data matching/data mining

The ALRC has proposed that the Office of the Privacy Commissioner should provide guidance on the privacy implications of data matching.

Guidance proposed will be similar to those currently regulating the public sector, which includes items such as:

- *Public notice of proposed data-matching and data-mining programs outlining the nature and scope of a data-matching program;*
- *Opportunity for affected individuals to comment on matched information if action may be taken on the basis of it;*
- *Destruction of unmatched personal information; and*
- *Restrictions on creating new databases from information about individuals whose records have been matched.*

The ALRC is concerned that data matching and data mining threaten privacy by:

- *Revealing new information about an individual without their knowledge or consent*
- *Profiling of individuals*
- *Difficulty for individuals accessing the new data-set without knowledge that such a data-set was compiled*
- *Accuracy of matched data*
- *Security of large amounts of data collected for the purposes of data matching or data mining. (proposal 7-6)*

In ANZ's opinion, data matching and analysis in the private sector is appropriately governed by the National Privacy Principles (NPPs). The NPPs restrict the application of data matching and analysis and its outputs by reference to the primary purpose of collection. ANZ believes it would be worthwhile for the ALRC to look further at the NPPs in relation to data matching and mining activities as opposed to trying to adapt the public sector guidelines to data mining and matching activities.

Proposed public notice of data-matching and data-mining programs

The proposed Public notice of proposed data-matching and data-mining programs, outlining the nature and scope of a data-matching program is cause for some concern. ANZ's fraud management program relies heavily on the ability to profile customer account activity against rules, typologies and established customer behaviours to detect and prevent fraud.

While people engaged in fraudulent behaviour are likely to be aware of this practice, public notices advising of this and other similar programs would have little benefit to the consumer.

Potential impact on Anti-Money Laundering and Counter Terrorist Financing Act

ANZ is concerned about the potential impact that any restrictions to data matching could have on both 'know your customer' (KYC) and transaction

monitoring requirements as set out in the *Anti-Money Laundering and Counter Terrorist Financing Act* (AML). Data matching across systems to form a holistic view of single customers is a fundamental requirement for businesses to achieve the KYC objectives. For businesses to identify abnormal and suspect transactions, customer profiling has to be done. Suspect transactions are generally viewed as a trigger for further customer due diligence. Providing customers with an opportunity to comment on matched information (as proposed by the ALRC) could undermine these profiling exercises more broadly.

Security of data

ANZ has stringent user controls in place to ensure that only authorised employees are able to access customer data for matching and mining exercises. Information produced by these processes is regularly collated into a summarised format, with only limited customer information available. If a compromise to security were to occur, the information would be of little use to someone not familiar with the matching exercise and it would be virtually impossible to match data back to the originating source.

In terms of protection and destruction of personal information, ANZ is of the view that current obligations governing the protection of personal information are working well and that any move to change them would be unnecessary. ANZ is acutely aware of need to maintain robust processes and systems to ensure information security. In addition, these models represent proprietary information which ANZ would not wish to disclose.

Under the national privacy principles, businesses are already required to ensure personal information is destroyed or permanently de-identified when no longer required. From ANZ's perspective, this principle is working well in practice.

Accuracy of matched data

Data matching is a tool that enables organisations to provide more targeted services to customers. In ANZ's experience, customers expect to be made aware of new products that might suit their individual needs. Given the objectives of data matching, it is in the organisation's best interests to ensure that only accurate and relevant information is collected and that this information is kept as up to date as possible.

Data matching forms an integral part of the way ANZ delivers improved services to customers by informing them of products that may better suit their financial needs. ANZ's Privacy Policy informs customers that ANZ may use personal information to assist it in providing information to customers about a product or service. Our customers are able to opt out of receiving marketing material if they wish.

Data Breach Notifications

ALRC proposes to introduce a new part to the Privacy Act:

- *To require organisations to notify the Privacy Commissioner and individuals where access to personal information has been acquired (or where reasonably believe to have been acquired) by an unauthorised person, and where the organisation or Privacy Commissioner believes it could lead to a 'real risk of serious harm' to affected persons.*
- Not required to notify any affected individual where:

- *Specified information is 'encrypted adequately'*
 - *Specified information was acquired in good faith by an employee or agent, where organisation otherwise acting for a purpose permitted by the proposed UPPs, provided the information is "not used or subject to further unauthorised disclosure"*
 - *Privacy Commissioner does not consider notification to be in the public interest*
- *Failure to notify Privacy Commissioner may attract a civil penalty. (proposal 47-1)*

ANZ welcomes the ALRC's recognition that breach reporting obligations should be subject to the materiality threshold of 'real risk of serious harm'.

While the Privacy Act does not impose an obligation on agencies and organisations to notify individuals whose personal information has been compromised, ANZ already has in place a practice of notifying customers about unauthorised access.

In terms of the ALRC's reference to 'adequate encryption', ANZ is of the view that there would need to be some form of certification of an organisation's encryption standard to ensure that it provides adequate security.

ANZ shares personal information about its customers with a number of third parties which support ANZ's business processes. Where third party breaches occur, ANZ believes flexibility should be retained (determined by relevant contract) as to whether the organisation, or third party, should be responsible for:

- Determining whether a breach is capable of causing serious harm; and
- Completing notification procedures. Furthermore, where one party has completed notification procedures, it should be deemed that all parties have discharged this obligation in full.

Consent

The OPC should provide further advice about what is required of agencies and organisations to obtain an individual's consent for the purposes of the Privacy Act. This guidance should: (a) cover consent as it applies in various contexts; and (b) include advice on when it is and is not appropriate to use the mechanism of 'bundled consent'. (proposal 16-1)

ANZ is of the firm view that bundled consent is necessary for reasons of practicality and efficiency. In particular, given the nature of a banking relationship, a bank has multiple interactions with an individual client which requires clients' information to be handled multiple times by various parts of the organisation. ANZ uses personal information from millions of customers in a number of different ways. For example, ANZ may use customer information to build scorecards, to effect payments or to assess an individual's capacity to repay a loan. ANZ takes its duty of confidentiality in relation to the use of personal information very seriously.

Once a banking relationship is established, customers generally expect ongoing communication from their bank. ANZ communicates regularly with its customers about services and products that may be beneficial to a customer's circumstance, except of course where customers have told us they do not wish to receive such information. ANZ believes that guidelines governing the use of bundled consent

have been developed to the point where they would have little practical use if the practice were restricted any further.

As explained in ANZ's February 2007 submission, for financial institutions, very few data uses and disclosures fall outside the primary purpose of collection. ANZ has limited its consent to the minimum necessary to run its business and provide services. ANZ ensures consents are obtained only when they are needed, generally at the application stage, and has sought to remove terms and conditions wherever practicable. Further consent is obtained only for uses which are genuinely unrelated to the primary purpose.

Data Security

ALRC has proposed the 'Data Security' principles to require an organisation to take reasonable steps to ensure personal information it discloses to a person, pursuant to a contract or otherwise in connection with the provision of a service to the organisation, is protected from being misused or disclosed without consent by that person. (proposal 25-2)

ANZ is of the view that where a third party has agreed to undertake 'reasonable steps' to protect personal information, that this should adequately satisfy this proposed requirement. There should not be a requirement for the organisation that supplied the information to the third party to conduct any review, audit or physical inspection of that third party to ensure the party can deliver on contractual promises, although in some cases an organisation may decide that it would be appropriate to ensure that a third party has appropriate data security measures in place. As an overriding principle, ANZ would not enter into a contractual arrangement with a third party if it believed the party did not have adequate information security processes in place.

In this context, providing 'reasonable steps' have been taken in disclosing personal information to a responsible third party, ANZ believes it would be unreasonable for an organisation to be held liable for any losses or damages arising directly or indirectly as a result of a breach by the third party.

Access and Correction

ALRC has proposed 'Access and Correction' principle should provide that where, in accordance with this principle, an organisation has corrected personal information it holds about an individual, and the individual requests that the organisation notify any other entities to whom the personal information has already been disclosed prior to correction, the organisation must take reasonable steps to do so, provided such notification would be practicable in the circumstances. (proposal 26-4)

With regards to the Access Principle, ANZ believes that current privacy principles provide customers with sufficient access to their personal information. ANZ employs good practices in providing customers access to their personal information. For example, in circumstances where there is an exception to the general provision granting a right of access ANZ takes reasonable steps to meet the needs of both ANZ and its customers.

In terms of the ALRC's proposed Correction Principle, ANZ currently takes reasonable steps to ensure personal information about the individual is accurate, complete and up-to-date at the time of collecting, using or disclosing the information. ANZ currently undertakes to promptly update any information that is inaccurate, incomplete or out of date. In those circumstances where ANZ

disagrees with a request to correct personal information, the individual has the right to request that a statement be attached to their information.

ANZ believes that if this proposal is adopted then it should apply only where inaccuracies are considered by a reasonable person to be material and would be practicable in the circumstances. The requirement to track all personal information disclosed to third parties, and to track whether all third parties have been notified of an update, would be unduly onerous and involve significant cost.

In this context, it should be noted that not all personal information is held on computer systems. While the majority of personal information held by ANZ or its contracted third parties is held electronically, some information is held in hard copy, meaning that it is sometimes difficult to identify all records kept on a customer in a timely manner.

ANZ agrees with the ALRC proposal that the Privacy Commissioner should provide clear guidance on the meaning of 'reasonable steps'.

Transborder Data Flows

ALRC is proposing that an organisation within Australia can only transfer personal information to recipient outside Australia if one of the following conditions is met:

- a) The organisation reasonably believes the recipient is subject to a law, binding scheme or contract which effectively upholds UPPs (or substantially similar); or*
- b) The individual consents to transfer; or*
- c) The organisation continues to be liable for any breach by recipient, and:
 - Individual would reasonably expect the transfer, and the transfer is necessary for performance of the contract between the organisation and the individual;*
 - Individual would reasonably expect the transfer, and the transfer is necessary to implement pre-contractual measures requested by individual;*
 - Transfer is necessary for the conclusion of performance of contract concluded in the interest of the individual, between the agency or organisation and a third party;*
 - All the following apply: the transfer is for benefit of the individual, it is impractical to obtain consent of the individual to transfer, and if it were impracticable to obtain such consent, the individual would likely to give it; or*
 - Before the transfer took place, the organisation took reasonable steps to ensure that the information will not be dealt with by the recipient of the information inconsistently with the proposed UPPs.**

ANZ supports the principle that bank customers should have information about the transfer of personal information overseas.

From ANZ's perspective, the current requirements governing the transfer of data overseas are working well. In its February 2007 submission to the ALRC, ANZ stated that it did not see the need to change current requirements governing transborder data protection, particularly where the information is transferred to a subsidiary located overseas. ANZ remains of this view.

ANZ agrees with ALRC's view that requiring written notification or consent each time an agency or organisation transfers an individual's personal information overseas would result in an unjustified compliance burden. As outlined in its February submission, ANZ stated that it would be supportive of notifying customers of the transfer of personal information overseas in its privacy policy. Such a notification could outline the circumstances in which personal information is sent overseas and the types of information security controls that have been put in place to protect that information.

While ALRC's proposal regarding when an agency or organisation may transfer personal information about an individual to a recipient (other than the agency, organisation or individual) outside Australia would preserve ANZ's ability to send personal information about an individual offshore, ANZ believes it would be unreasonable for an organisation to 'continue to be liable' for breaches by a third party of the proposed UPPs. Where third party breaches occur, ANZ believes flexibility should be retained (determined by relevant contract) as to whether the organisation, or third party, should be responsible for:

- Determining whether a breach is capable of causing serious harm; and
- Completing notification procedures. Furthermore, where one party has completed notification procedures, it should be deemed that all parties have discharged this obligation in full.

Rights of Access, Complaint Handling and Penalties

ALRC proposes that the Privacy (Credit Reporting Information) Regulations should provide that the information to be given if an individual's application for credit is refused based wholly or partly on credit reporting information should include any credit score or ranking used by the credit provider, together with explanatory material on scoring systems, to allow individuals to understand how the risk of the credit application was assessed. (proposal 55-3)

ANZ is of the view that this proposal, particularly the inclusion of a credit score, would be unlikely to lead to an individual being any better informed about how the risk of the credit application was assessed. The main reason for this is that financial institutions have developed proprietary systems which rely on criteria specific to the organisations' own credit assessment requirements. Many of these systems do not use the same terminology or the same scale for assessing customer scores. Therefore, knowing a score with one organisation is likely to serve only as a guide to whether or not the individual would (or would not) obtain credit from another organisation.

ANZ has invested heavily in developing its credit assessment models and would not wish to disclose in a credit report any proprietary information related to these models. ANZ is of the view that a balance would need to be found between trying to provide an individual with meaningful information about their credit application assessment and to adequately protecting the proprietary nature of an organisation's assessment models.

The ALRC proposes that the Privacy (Credit Reporting Information) Regulations should provide that credit providers have an obligation to provide evidence to individuals and dispute resolution bodies to substantiate disputed credit reporting information, such as default listings, and that if the information is not provided within 30 days the credit reporting agency must delete the information on the request of the individual concerned. (proposal 55-7)

ANZ is supportive of this proposal but believes the proposed 30 day requirement to provide information is onerous. ANZ is of the view that setting a 60 day time limit would provide a more realistic timeframe in which to address the ALRC's proposed changes.

Direct marketing

The ALRC recommends the introduction of a new Privacy Principle dealing specifically with direct marketing. The ALRC proposes that the principle implement an 'opt out' policy, requiring organisations to give effect to requests from individuals to not receive direct marketing from the organisation.

The ALRC proposes that an organisation must not use or disclose personal information about an individual for the primary purpose or a secondary purpose of direct marketing unless all of the following conditions are met:

- (a) the individual has consented, or both of the following apply:
 - (i) the information is not sensitive information; and*
 - (ii) it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure; and**
- (b) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and*
- (c) the individual has not made a request to the organisation not to receive direct marketing communications, and the individual has not withdrawn any consent he or she may have to the organisation to receive direct marketing communications; and*
- (d) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications.*

The ALRC also proposes that organisations must comply with a request not to send direct marketing communications within a reasonable period of time and must take reasonable steps (when requested by the individual) to advise the individual from where it acquired the individual's personal information.

ANZ broadly supports this proposal but believes the current 'opt out' provisions for customers to decline from receiving marketing material from the bank are working well. As outlined in ANZ's February 2007 submission, ANZ communicates regularly with its customers about services and products that may be beneficial to a customer's circumstance. ANZ Customers can contact ANZ at any time if they do not want to receive marketing information from ANZ. To date, around eight per cent of ANZ customers have elected not to receive direct marketing material from the bank (this figure refers to ANZ personal customers only).

Identity verification

The ALRC asks if the use and disclosure of credit reporting information for identity verification purposes is not authorised under the proposed Privacy (Credit Reporting Information) Regulations, what other sources of data might be used by credit providers to satisfy obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) and similar legislation.

In order to achieve an appropriate balance between business process efficiency and consumer privacy protection, ANZ is of the view that credit reporting information should be available for the purposes of identity verification for both credit and retail based products. The possibility of using several data sources electronically to create an identity match represents a real benefit, particularly for those businesses where face-to-face interaction with customers is minimal or non-existent. It would also benefit remote customers who do not have access to a bank branch and must use alternative and more onerous methods of providing their identification.

Access to credit reporting information for electronic identity verification would also facilitate the 'safe harbour' procedure contained in the AML/CTF Rules. (The 'safe harbour' electronic verification procedure requires ANZ to verify the customer's name and customer's residential address using electronic data from at least two separate data sources; and either their date of birth or transaction history for at least the past three years.)

In response to ALRC's question regarding other sources of data which might be used by credit providers to satisfy obligations under the AML/CTF Rules, ANZ is not aware of any databases other than the credit database that can be readily interrogated by reporting entities to satisfy the relevant obligations.

Employee privacy

ALRC proposes that the Privacy Act be amended to remove the employee record exemption. The ALRC considers that employee records contain significant amounts of personal information and that there is a potential for individuals to be harmed by misuse or inappropriate disclosure of their privacy records. In addition, the ALRC notes that there is no sound policy reason why privacy protection for employee records is only available to public sector employees and not private sector employees. To this end, the ALRC proposes that information about employees be subject to the UPPs and to other privacy obligations. (proposal 36-1)

While ANZ observes good privacy practice in relation to its employees, it is of the view that there remains a need for an employee record exemption.

However, if the employee record exemption were removed, ANZ would agree with the ALRC proposal that the Privacy Act should also be amended to provide that an agency or organisation may deny a request for access to evaluative material, disclosure of which would breach an obligation of confidence to the supplier of the information. ('Evaluative material' for these purposes means evaluative or opinion compiled solely for the purpose of determining the suitability, eligibility, or qualifications of the individual concerned for employment, appointment or the award of a contract, scholarship, honour, or other benefit.)

New right of action: Invasion of Privacy

The ALRC has proposed the introduction of a tort of invasion of privacy, actionable where: there has been an interference with an individual's home or family life; an individual has been subjected to unauthorised surveillance; an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; or sensitive facts relating to an individual's private life have been disclosed; and the act complained of is sufficiently serious to cause substantial offence to a person of 'ordinary sensibilities'.

In pursuing the recovery of debts and the enforcement of security rights against individuals, it is difficult to avoid some direct interaction with home or family life. The conduct of debt recovery is regulated by the Code of Banking Practice and the Guidelines published by the Australian Securities and Investments Commission. Both the Code of Banking Practice and Guidelines provide guidance on debt recovery so as to minimise unnecessary and inappropriate interference with home life and personal dignity. ANZ is of the view that these debt collection and security enforcement arrangements are working well in practice and that they should remain outside of the scope of the proposed statutory action for invasion of privacy.

Deceased individuals

The ALRC recommends extending the application of Privacy law to personal information of deceased persons, including the rights of access and correction.

ANZ is of the view that financial information should not become subject to a right of access to any individual other than those with legal rights to administer the financial affairs of deceased estates.

Comprehensive Credit Reporting

ANZ supports in principle ALRC's proposal to move towards a system of more comprehensive credit reporting. ANZ agrees with the ALRC position that comprehensive (or positive) credit information should increase the efficiency of credit markets and improve risk assessment by credit providers, providing that a number of key issues are properly dealt with in any credit reporting model.

As the ALRC correctly points out, any expansion in the categories of personal information that may be collected for credit reporting purposes should not be considered in isolation from other aspects of the privacy regulation of credit reporting. The design of the system will have a strong bearing on the social and economic outcomes of a comprehensive credit reporting system.

While ANZ is of the view that the ALRC has proposed an appropriately balanced approach that promotes both credit market efficiency and privacy protection, there are some aspects of the proposal which require further consideration. The discussion below responds to those elements of the ALRC paper which are of particular importance to ANZ's operations.

ANZ believes it would be prudent to review the credit reporting regulations after they have been operating for a period of time. ANZ supports the ALRC proposal that credit reporting regulations be reviewed after five years of operation.

ANZ considers data quality an important aspect of any credit reporting system and supports the development of industry standards for data quality under a comprehensive credit reporting system. Under the current system, negative credit data is reported on an 'exception' basis. However, positive credit reporting would require a regular feed of 'current' data, which in itself may improve the quality and accuracy of the information held by credit reporting agencies.

ANZ considers that credit reporting should be supported by an accessible dispute resolution scheme, such as the Banking and Financial Services Ombudsman. This is necessary regardless of the type of credit reporting system. The Australian Retail Credit Association (ARCA) is working towards producing a Code of Conduct for participants in credit reporting, a key part of which is the establishment of a dispute resolution scheme which is likely to leverage off existing schemes.

ANZ supports the ALRC proposal that credit reporting agencies and credit providers should develop, in consultation with consumer groups and regulators, including the OPC, an industry code dealing with operational matters such as default reporting obligations and protocols and procedures for the auditing of credit reporting information. However, in developing any Code, it will be important to ensure that consumer and privacy groups are thoroughly consulted and that their concerns surrounding data protection, privacy safeguards, data quality, complaints handling/dispute resolution and governance are adequately addressed.

A self-regulatory model with adequate governance through an advisory body with representation from relevant stakeholder groups would be an appropriate approach to regulating credit reporting more broadly. The regulatory framework for a comprehensive credit reporting system need not be unnecessarily burdensome on credit providers but must also provide protection for consumers and their privacy. The Australian Retail Credit Association (ARCA), in consultation with relevant stakeholders, is working towards producing a Code of Conduct for participants in credit reporting.

New categories of personal information

The ALRC has proposed that the Privacy regulations should permit the inclusion in credit reporting files of the following categories of personal information in addition to those currently permitted, including:

- (a) the type of each current credit account opened*
- (b) the date on which each current account was opened;*
- (c) the limit of each current account; and*
- (d) the date on which each credit account was closed.*

ANZ supports this proposal but is of the view that the inclusion of an additional category relating to repayment history over the last 24 months would significantly enhance the accuracy and utility of the proposed credit reporting system. The inclusion of the information proposed by the ALRC will improve marginally the quality of lending decisions and pricing of risk. However, in order to gain a more accurate and complete assessment of a customer's credit worthiness it is important to have some level of historical repayment data. For this reason, ANZ is of the view that the ALRC should consider including an additional category of personal information relating to an individual's repayment history.

Data Reciprocity

The credit reporting industry code should provide for access to information on credit information files according to principles of reciprocity. That is, in general, credit providers only should have access to the same categories of personal information that they provide to the credit reporting agency. (proposal 51-2)

ANZ welcomes ALRC's proposal that the credit reporting industry code should provide for access to information on credit information files according to principles of reciprocity. ANZ firmly supports the ALRC view that credit providers should have access only to the same categories of personal information (ie. on a like for like basis) that they provide to the credit reporting agency. Furthermore, the principle of reciprocity should provide a strong incentive for lenders to participate in a comprehensive credit reporting system.

ANZ agrees with the ALRC's view that credit providers and industry associations should take responsibility for deciding how information sharing should proceed

within the framework provided by legislation. In this regard, further examination of overseas models would be needed to determine which features would suit the Australian environment.

Collection of Credit Reporting information

ALRC proposes that the Privacy (Credit Reporting Information) Regulations provide that, at or before credit report information is collected about the individual, the credit provider must take reasonable steps to ensure the individual is aware of:

- a) The facts and circumstances of collection;*
- b) Credit provider's and credit reporting agency's identity and contact details;*
- c) The fact that the individual is able to gain access to the information*
- d) Main consequences of not providing information;*
- e) Types of people, organisations, agencies, or other entities to whom the credit provider usually discloses credit reporting information;*
and
- f) Avenues of complaint regarding handling and collection of information - (proposal 52-9)*

As outlined in ANZ's June 2007 submission to the ALRC, access to comprehensive credit information should occur only with the express consent of consumer applicants and be limited to credit providers assessing a credit application and credit reporting agencies. However, it is important to note that while a consumer may be able to refuse consent, a credit provider is unlikely to extend credit if it is unable to make an adequate risk assessment based on all the available information.

Notwithstanding, ANZ is of the view that the obligations already imposed on organisations at the time of collection of personal information adequately inform the individual about how their personal information is used and how they can go about resolving a concern or complaint.

In almost all ANZ customer interactions, the facts and circumstances of information collection are made clear. Where this proposal might apply, such as where ANZ collects information via cookies or other technologies, ANZ already discloses its practice in its website privacy statement. As outlined in ANZ's February 2007 submission to the ALRC, matters that must be disclosed should be limited to information that is absolutely essential to the consumer at the beginning of their relationship with the organisation.

As highlighted in the ALRC issues paper 31, lengthy privacy notices may not adequately inform the consumer, as they can be overwhelmed or deterred from reading them given the amount of information provided. Adding further information to that which is already provided to consumers may not necessarily achieve the outcomes desired, including greater consumer awareness about the information being collected about them. In this regard, ANZ believes its Privacy Policy (available at www.anz.com) provides customers with a comprehensive and straightforward guide to ANZ's privacy obligations.

ANZ is of the view that an individual should be provided with credit reporting agency details upon request; terms and conditions should continue to disclose that information which may be disclosed to credit reporting agencies, but without specifying which agencies.

Direct marketing

ALRC proposes that the Privacy Regulations should prohibit the use or disclosure of credit reporting information for the purposes of direct marketing (proposal 53-3).

ANZ agrees with the ALRC proposal that credit reporting regulation should ensure that credit reporting information should not be used for direct marketing. As a general principle, ANZ would not support unrestricted access to personal information for marketing purposes and only after an individual has given their consent.

The ALRC asks whether credit providers should be permitted to use credit reporting information to pre-screen credit offers. If so, the ALRC asks whether credit providers should be required to allow individuals to opt out, or whether credit providers should only be permitted to engage in pre-screening if the individual has expressly opted in to receiving credit offers. (Question 53-2)

ANZ is of the view that credit providers should be permitted to use credit reporting information to pre-screen credit offers and that credit providers should be required to allow individuals to opt out of pre-screening credit offers.

By pre-screening credit offers, credit providers can significantly reduce the volume of direct marketing of credit offers to individuals with poor credit histories. For example, in ANZ's experience, approval rates following pre-screening for customers applying for credit, can be up to four-fold higher than for non pre-screened data. At no point does ANZ have access to customer data used by the bureau as this is strictly protected by the bureau for privacy reasons.

ANZ regularly updates its customer exclusion rules against bureau data to ensure customers who have opted out or who have been recently had a credit application declined are excluded from future mailings.

Conclusion

Given the complex nature of many of the reform proposals and the potential impact they will have on many organisations, that there should be further opportunity for industry to be consulted on key proposals. ANZ would be pleased to meet with the ALRC to discuss this submission, particularly aspects relating to automated decisioning where we have expertise, in more detail and can be contacted as follows:

Ms Jane Nash
Head of ANZ Government & Regulatory Affairs
Level 22, 100 Queen Street
Melbourne VIC 3000
(03) 9273 6263
Jane.Nash@anz.com