AUSTRALIAN BANKERS' ASSOCIATION

Submission to

HOUSE OF REPRESENTATIVES

STANDING COMMITTEE ON LEGAL AND CONSTITUTIONAL AFFAIRS

INQUIRY INTO

PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000

May 2000

Australian Bankers' Association represents 25 authorised banks operating in Australia including the four large banks and regional banks.

ABA and its member banks participated extensively in the development of the National Principles for the Fair Handling of Personal Information that were first released by the former Privacy Commissioner in February 1998. ABA supports those principles. They were developed through a broad-based consultative process involving government, business, privacy and community interests.

ABA supported the Commonwealth Government's decision in December 1998 to support and strengthen self-regulation by the private sector on privacy protection through "light touch" legislation.

Along with a broad-based group of interested parties, ABA also participated in the Commonwealth Attorney-General's Core Consultative Group that assisted the Government in the development of the Privacy Amendment (Private Sector) Bill 2000.

The Bill and the National Privacy Principles are the product of unprecedented consultation with relevant stakeholders. The Bill is the culmination of a consultative incremental process since 1996.

Therefore, ABA submits that key policy settings leading to the introduction of the Bill should be left undisturbed. Central to this are the National Privacy Principles.

Related Entities Sharing Personal Information

A fundamental concept in the Bill is the ability of related companies in a corporate group to share and use customer information responsibly. This concept was embodied in the National Principles for the Fair Handling of Personal Information in a way that treated the group of related corporate entities as one organisation. Companies that comprise a bank group are required to remain as separate legal entities for legal and prudential reasons. Unlike some other businesses, a bank group's separate business units are not

permitted to sit within the single corporate entity that is the bank. Yet, the reality of the Australian financial system is that it comprises predominantly financial conglomerates. This was a key observation of the Wallis inquiry into the Australian financial system (see *Financial System Inquiry Final Report 18 March 1997* at 4.4.1 page 155)
The Bill seeks to enshrine this concept through the combination of clause 13B and National Privacy Principles 1.3, 1.5 and 2.1. However, we observe that the Bill does not recognise the conglomerate structure as the one organisation in the same way as that structure was recognised under the national Principles for the Fair Handling of Personal Information.

ABA accepts the notion that at the point personal information is first collected by an organisation from the individual concerned, the information is "tagged" with a primary purpose that stays with the information for the rest of its life in the organisation and its related entities. That primary purpose should be made known to the individual concerned under NPP 1.3 unless, of course, the purpose is plainly evident from the transaction being undertaken e.g. opening an account. Other contemplated disclosures or uses should also be disclosed. It is clear from the Explanatory Memorandum to the Bill that these disclosures should contain sufficient detail to help the individual to understand the types of persons in the organisation that may be handling the information. Also, by being more explicit the organisation can shape the expectation of the individual about what the information may be used for and to whom it will be disclosed. In particular the Explanatory Memorandum stipulates that where disclosures to related bodies corporate are contemplated that should be disclosed. This then satisfies the OECD principle that the individual must know data is being collected at the point of collection and successively through the further disclosures permitted between related entities in a corporate group (as one discloses the other collects).

ABA accepts that it is good business practice to make information handling practices transparent for consumers and that the Bill's provisions achieve an appropriate standard of transparency in this respect.

In helping consumers to understand the purposes of organisations when collecting and handling personal information and to help organisations better understand their responsibilities in this respect, the Bill should explicitly recognise that there may be more than one "primary" purpose or significant reason why personal information is first collected. These are pivotal concepts under the National Privacy Principles and, as such, should leave no room for doubt. If there is more than one significant purpose the organisation should be able to specify this so the customer is properly informed. If these expressions are left vague, this is likely to lead to arguments between organisations and their customers about which one of say three specified purposes is the "primary" purpose. Clarity in this respect is of benefit to all.

Dispute Resolution

The Bill recognises and supports the valuable contribution the private sector can make to ensuring that disputes between organisations and individuals about privacy are handled

independently, simply, cost effectively, free to the individual, flexibly and with a minimum of legal form and procedure. These characteristics of industry based customer dispute resolution schemes are the hallmarks of their success and wide ranging acceptance by consumers in other areas of dispute resolution. Typically, a dispute referred to such a scheme will be investigated and a conclusion reached on the propriety of the alleged conduct. In many cases disputes can be resolved without the need for any hearing involving the parties to the dispute. Schemes do not have the power to administer the oath and rely on astute evaluation of the law and the facts as provided to reach a conclusion. Under the Australian Banking Industry Ombudsman scheme, if a customer is not satisfied with the decision of the scheme he or she is not bound by it. Conversely, if the customer accepts the decision the bank is then bound to that decision.

Under the Bill, the ability of the Federal Court to review decisions of a dispute resolution scheme (code adjudicator) is likely to work against the interests of consumers. The Bill contemplates that code adjudicator decisions will be reviewable under the Administrative Decisions (Judicial Review) Act 1977 ("ADJR Act"). The grounds for review under the ADJR Act include:

- Breach of the rules of natural justice;
- Non-observance of procedures required by law to followed;
- Error of law; or
- Improper exercise of power including taking account of irrelevant factors or failing to take account of relevant factors.

It would seem inconsistent with the notion that the decision of a scheme that binds an organisation at the option of the complainant could conceivably be overruled by a later application under the Act by the complainant who believes the decision, with hindsight, was for example wrong in law. The organisation nevertheless remains bound.

Inevitably, the prospect of judicial review of scheme decisions will cause schemes to review their practices and procedures resulting in loss of flexibility, delay, increased legalism in both form and substance and an increase in the costs of running the schemes. The effectiveness of the schemes in delivering a result promptly and to the satisfaction of the complainant is likely to be adversely affected.

The problems and inefficiencies caused by the prospect of judicial review of scheme decisions could discourage some private sector bodies from making their schemes available for handling privacy disputes. This would place considerable burdens and costs on the Privacy Commissioner and his staff to handle such disputes instead.

If the objective is to ensure that private sector code adjudicators perform according to appropriate standards and are consistent in their approaches to the law, the Committee's attention is drawn to the criteria set out in clause 18BB of the Bill that the Privacy Commissioner must observe when approving a code adjudication mechanism.

ABA submits that there would be an ongoing obligation on code adjudicators to satisfy these criteria and that the power of revocation exercisable by the Privacy Commissioner (clause 18BE) would act as a strong incentive for these standards to continue to be met. As such, code adjudicators become accountable to the Privacy Commissioner for their performance rather than the Court. The Privacy Commissioner is in turn accountable to the Parliament.

Therefore, ABA submits that the proposal in the Bill for private sector code adjudicator decisions to be made subject to judicial review under the ADJR Act should be abandoned.

Under clause 18BF (1)(b) of the Bill, the Privacy Commissioner would have power to issue guidelines relating to making and dealing with complaints. This power seems to be exercisable in the unfettered discretion of the Privacy Commissioner. There is no explicit direction or requirement for the Privacy Commissioner to consult with anyone in formulating such guidelines. By force of clause 18BB(3) of the Bill, such guidelines would have effect in law because the Privacy Commissioner could not approve a complaint handling mechanism or body unless he or she is satisfied those guidelines are met. This is, in effect, an unfettered legislative power conferred on the Privacy Commissioner.

ABA supports the Privacy Commissioner having the necessary powers to ensure that codes and complaints handling arrangements are adequate. ABA believes such powers should not be delegated without guidance to the Privacy Commissioner on how those powers should be exercised.

Data Collected before the Commencement

The Bill takes a practical, realistic approach to personal information that organisations collect before the Bill's provisions come into effect (existing data). It follows the approach taken in the National Principles for the Fair Handling of Personal Information. Also, it follows, in the main, the approach taken in the Privacy Act when it first commenced to apply to government agencies (see section 15 Privacy Act 1988). Under the provisions of the Bill, existing data will be subject to the data security, data quality (if used or disclosed), openness, unique identifiers and transborder data transfer principles. The Bill does not extend the use and disclosure principles to existing data because the task of combing through existing data bases and trying to ascribe a primary purpose to the data, if possible at all, would be an immense and costly task. Banks have millions of customers many of whom have more than one account or product relationship with them. Equally, approaching each customer for consent would be very onerous with little prospect of a response one way or the other.

Also, customer data can become outdated very quickly. It would be pointless to oblige organisations to embark upon the tasks described above in such circumstances.

It is worth noting that banks are bound by a duty to keep the affairs of their customers confidential. This duty is unaffected by the Bill's provisions. Banks would not be able to disclose existing data about their customers to third parties unless the customer had consented or unless one of the other exceptions to the duty were to apply (i.e. disclosure under compulsion of law, disclosure pursuant to a public duty or disclosure where the bank's vital interests are involved such as prosecuting or defending a legal action).

For similar reasons the access and correction principle should not apply to existing data. The potential for customers to demand production of all data held about them would again be an extremely time and labour intensive task particularly when it is considered that large stocks of data are held securely in manual storage off-site in most cases.

Exemptions

The Long Title to the Privacy Act 1988 states its purpose as "An Act to make provision to protect the privacy of individuals, and for related purposes". It follows that the exemption of some organisations from the legislation points to a failure of the Act in meeting its stated purpose. Logically, if an organisation collects and handles personal information and therefore has the potential to interfere with the privacy of the individual, that organisation should be covered by the legislation.

Difficulties for members of the public where certain businesses are exempted from the provisions of the legislation will include their ability to identify those businesses that are covered by the legislation and those that are not. A business could actively promote its information handling practices but nevertheless not incur the consequences of non-compliance that those that are bound by the legislation would incur.

Exemptions could lead to certain businesses being disadvantaged. The public may choose not to deal with those businesses because they are not covered by the legislation. Companies that are bound by the legislation may choose not to outsource functions to entities that are not bound so as to protect the customers of the outsourcing company.

It is observed that the turnover threshold for exemption of small businesses under the proposed legislation is $3m.

The Bill and the National Privacy Principles have been framed to support and strengthen self-regulation. They are, in the main, "light touch" provisions that, if they retain their "light touch" character, should not carry significant compliance costs for small business operators.

Conclusion

The Bill's response to privacy protection in the private sector is balanced as a result of extensive consultation. Subject to the comments we respectfully make in this submission, we believe the approach now should be to move the Bill through its legislative stages as

quickly as possible retaining key policy settings whilst ensuring that consumer benefits and the costs of compliance are appropriately weighted.