PRIVACY LAW ISSUES — REFORM PROPOSALS AND THEIR IMPACT ON THE FINANCIAL INDUSTRY

ROS GRADY*

Partner
Mallesons Stephen Jaques, Solicitors, Melbourne

INTRODUCTION

With the announcement by the Prime Minister on 21 March 1997 that the Commonwealth Government will not be implementing privacy legislation for the private sector many of you may be wondering whether there remain any privacy law issues of concern to the finance industry. The answer is a most definite "yes".

My principal focus today is to examine the privacy issues of most concern to credit providers in Australia today and then examine the ways in which these issues might best be dealt with in the future.

CURRENT PRIVACY REGULATION IN AUSTRALIA

Our first task is to look at the many different forms of privacy regulation currently in Australia.

It will be seen that the different forms of regulation individually give rise to issues and together create a regime which involves a number of inter-connecting layers not all of which impose consistent obligations. This disuniformity has, of course, the potential to increase if the States enact their own privacy legislation and if increased use of electronic banking techniques means credit providers have to also cope with international privacy rules.

The current scheme of privacy regulation in Australia is principally governed by:

- the common law which imposes a banker's duty of confidentiality;
- equitable duties of confidence;
- duties applicable to fiduciary relationships;
- Part IIIA of the Privacy Act 1988 (Commonwealth) (Privacy Act);

---

* With the assistance of Paula Murphy, Senior Associate.

- State privacy legislation, including the Privacy Committee Act 1975 (New South Wales), Invasion of Privacy Act 1971 (Queensland), Fair Trading Act 1987 (South Australia) and the Credit Reporting Act 1978 (Victoria); and

- various industry codes of practice containing confidentiality provisions including the Electronic Funds Transfer Code of Conduct, the Code of Banking Practice, the Credit Union Code of Practice and the Building Society Code of Practice. There are also codes of practice dealing with the issue of privacy which apply to electronic commerce. These will be discussed in the section of this paper dealing with that issue.

- I turn to look at some of those issues in more detail.

DUTIES OF CONFIDENCE AT COMMON LAW AND IN EQUITY

Nature of duties

A banker may be subject to:

- an equitable duty of confidence which applies to information which is of its nature confidential and which is imparted in circumstances where the recipient could reasonably expect to have realised that the recipient was under an obligation to keep the information confidential;[1] and

- a fiduciary relationship which exists between banker and customer in certain circumstances – for example where the bank takes on a role of an investment adviser or otherwise provides a service where the customer is clearly reliant on the bank's advice.[2]

However, the leading authority in Australia on a banker's duty of confidentiality is the English case of *Tournier v National Provincial and Union Bank of England*[3] (*Tournier*).

In summary, it was held in *Tournier* that it is an implied term of the banker-customer contract that the banker has a duty of confidentiality regarding a customer's account and matters relating to it. It is not an absolute duty as it is qualified by the following four exceptions:

- where disclosure is under compulsion of law;

- where there is a duty to the public to disclose;

- where the interests of the bank require disclosure; and

- where the disclosure is made with the express or implied consent of the customer.

I turn to briefly consider each of these exceptions.

---

1 *Castrol Australia Pty Ltd v Emtech Associates Pty Ltd* [1980] 51 FLR 184.

2 *Commonwealth Bank v Smith* (1991) 102 ALR 453 and *Hospital Products Ltd v United States Surgical Corporation* (1984) 156 CLR 41.

3 [1942] 1 KB 461.

Disclosure under Compulsion of Law

The examples given in *Tournier* of this exception were:

- "an order under the Banker's Books Evidence Act";[4] and
- an order "to answer questions in the law Courts".[5]

There are numerous other examples that can be cited of disclosures which might be made by a banker under compulsion of law. For example:

- disclosures made under the Consumer Credit Code;[6]
- disclosure pursuant to a search warrant;[7]
- disclosure to the Commissioner of Taxation under sections 263 and 264 of the Income Tax Assessment Act 1936 (Commonwealth);[8]
- disclosure of suspect and significant cash transactions to the Australian Transaction Reports and Analysis Centre (AUSTRAC) under the Financial Transaction Reports Act 1988 (Commonwealth);
- disclosure pursuant to the information powers contained in the Proceeds of Crime Act 1987 (Commonwealth);[9]
- disclosure pursuant to a notice served by the Australian Competition and Consumer Commission under section 155 of the Trade Practices Act 1974 (Commonwealth);
- disclosure to the Australian Securities Commission under the investigation powers contained in Part 3 of the Australian Securities Commission Act 1989 (Commonwealth); and
- disclosure to a trustee in bankruptcy of the existence of a bank account held by an undischarged bankrupt under section 125 of the Bankruptcy Act 1966 (Commonwealth).

---

4 Per Bankes LJ at page 473.

5 Per Scrutton LJ at page 481.

6 For example section 34(1) of the Consumer Credit Code requires a credit provider, at the request of a debtor or guarantor, to provide a statement of current balance to the debtor's account, any amounts credited or debited during the period specified in the request, any amounts overdue and when any such amount became due and any amount payable on the date it became due. Section 51(1) further provides that, before the obligations under a credit contract are secured by a guarantee, a credit provider must give to the prospective guarantor a copy of the contract document and the credit contract or proposed contract document. Failure to do so renders the guarantee unenforceable under section 51(2).

7 See, for example, section 3E(1) of the Crimes Act 1914 (Commonwealth).

8 See, for example, *Simionato Holdings Pty Ltd v Federal Taxation Commissioner (No 2)* 95 ATC 4720 at page 4727 where it was held that section 263 powers could be used to obtain documents from a bank for use in proceedings to recover unpaid tax.

9 See, for example, section 73 which provides for Supreme Court orders to be made directing a financial institution to give information to a law enforcement authority.

Disclosure on the Basis of a Duty to the Public

An explanation of this qualification to a banker's duty of confidentiality was given by Bankes LJ in *Tournier* as follows:

> "Many instances of [this exception] might be given. They may be summed up in the language of Lord Finlay in *Weld-Blundell v Stephens* [[1920] AC 956, 965] where he speaks of cases where a higher duty than the private duty is involved, as where 'danger to State or public duty may supersede the duty of the agent to its principal'."[10]

Notwithstanding these comments there is still a large deal of uncertainty regarding the scope of this exception.

Weerasooria in *Banking Law and the Financial System in Australia*[11] concludes in relation to this exception:

> "While the rights that are disclosed under this exception should not be lightly assumed, it would appear that it would apply in the following cases:
>
> - during time of war when the customer's dealings indicate that he is trading with the enemy;
> - during time of national emergency where a customer is reasonably suspected of treasonable activities against the State;
> - to prevent the perpetration or aid in the detection of serious frauds and crimes."[12]

In further academic comment, Walter and Erlich have suggested that where bankers are involved the judiciary may develop a test to weigh-up whether the disclosure was justified. Walter and Erlich consider the following factors would be relevant to such an assessment:

- whether the facts in front of the court display a situation a reasonable banker would understand to be one that would be in the public interest to disclose;
- whether clear, real and extensive danger to the public exists;
- whether the sole purpose for releasing the information was in the public interest and not a collateral purpose;
- whether the bank has carefully considered whether its action would be constructive and in the public interest;
- a lack of alternatives for the bank to pursue; and
- whether the bank weighed-up and balanced the harm that might flow from the disclosure, directly and indirectly.[13]

Weaver and Craigie suggest that, in the absence of any clear authority on this exception, the warning given by Sir John Paget in relation to its use remains as valid today as it was when he

---

10 Per Bankes LJ at page 473.

11 Third edition, 1993.

12 Weerasooria, *Banking Law and the Financial System in Australia*, third edition, 1993 at page 440.

13 "Confidences – Bankers and Customers: Powers of Banks to maintain Secrecy and Confidentiality", Walter and Erlich (Walter and Erlich) 63 *ALJ* 416 at page 404.

delivered it in 1924. "It would be inadvisable for a banker to exercise his private judgement in such matters at the expense of the customer."[14]

Disclosure in Interest of a Bank

Bankes LJ in *Tournier* stated in relation to this exception that a "simple instance ... is where a bank issues a writ claiming payment of an overdraft stating on the face of the writ the amount of the overdraft".[15]

Scrutton LJ also referred to the overdraft example.[16] I am not aware of a reported case directly on this point in Australia. The English case of *Sunderland v Barclay's Bank Ltd*[17] is relevant but has not been judicially considered in Australia.[18] It was held in that case to be in the bank's interest for the bank to disclose confidential information in relation to a demand for an explanation of why Mrs Sunderland's cheques had been dishonoured. The bank in that case told Mr Sunderland in a telephone call (which had been initiated by Mrs Sunderland) that the majority of the cheques that passed through his wife's account were in favour of bookmakers. The plaintiffs' claim was dismissed on the basis that the interests of the bank required the disclosure and, in any event, Mrs Sunderland had impliedly consented to disclosure by asking her husband to speak to the bank.

Disclosure by Express or Implied Consent

It will usually be clear when a bank is entitled to override its duty of confidentiality under the exception of express consent. A more difficult issue is where a bank seeks to rely on the exception of implied consent.

Guarantors

It has been argued by some commentators[19] that the information a bank can disclose to a guarantor or intending guarantor is an example of an exception of express or implied consent.

The Code of Banking Practice provisions dealing with guarantees seem to have little effect on the banker's duty of confidentiality. This is because the requirements relating to disclosure to a prospective or current guarantor are dependant on obtaining the consent of the borrower.[20]

However the effect of the Consumer Credit Code provisions on guarantees is different. Section 34(1) of the Consumer Credit Code provides that a credit provider must, at the request of a debtor or guarantor, provide a statement of the current balance of the debtor's account; any amounts credited or debited during the period specified in the request; any amounts overdue and when each such amount became due; and any amount payable on the date it became due. There are also provisions in section 34(2) in relation to the time within which the statement must be provided.

---

14 "Banker and Customer" Weaver and Craigie looseleaf service, page 2647.

15 Per Bankes LJ at page 473.

16 Per Scrutton LJ at page 481.

17 (1938) 5 LDB 163.

18 For discussion of *Sunderland v Barclay's Bank Ltd* see Walter and Erlich 63 *ALJ* 404 at page 416.

19 See Walter and Erlich 63 *ALJ* 404 at page 416.

20 See section 17 of the Code of Banking Practice.

Section 51(1) further provides that, before the obligations under a credit contract are secured by guarantee, the credit provider must give to the prospective guarantor a copy of the contract document of the credit contract or proposed credit contract and a document in the form prescribed by the regulations explaining the rights and obligations of the guarantor. Failure to do so renders the guarantee unenforceable.[21]

Section 163(1) also provides that other contracts and documents must be provided to a guarantor on request. These include any credit related insurance contract in the credit provider's possession and any notice previously given to the debtor under the Consumer Credit Code.[22]

Unlike the provisions of the Code of Banking Practice, the provisions in the Consumer Credit Code require disclosure by statutory force. There is no requirement that the consent of the affected borrower be obtained. It may accordingly be a defence to a claim for wrongful disclosure to a guarantor under the provisions of the Consumer Credit Code that disclosure was made under compulsion of law. However, an aggrieved borrower may argue that there was no compulsion of law in relation to at least the section 51 disclosures because the taking of the guarantee by the bank is a voluntary matter. To avoid any doubt on this issue, banks may wish to obtain an express consent to the relevant disclosures from a potential borrower as part of the credit approval process.

Bankers' opinions

The other area where this exception has been traditionally discussed is the convention of banks to give a banker's opinion.

It is a well established practice that a bank might give a banker's opinion concerning their customers' credit worthiness. Some debate has taken place in relation to whether the practice of giving a banker's opinion has reached a level whereby it is a trade custom and of which the customer is, or should be, aware and to which the customer gives implied consent. However some commentators believe that the giving of a banker's opinion is not well-known amongst customers and accordingly a customer's implied consent to the giving of such opinions cannot be drawn from the custom of bankers.[23] This issue has in any event been to some extent effected by the provisions of the Code of Banking Practice and the Privacy Act in relation to the giving of a banker's opinion (see discussion in "Disclosure by Consent and the Privacy Act" below).

PRIVACY ACT 1988 (CTH)

Private sector application

The Privacy Act applies to the private sector in only very limited areas. The areas involved concern tax file number information, credit reporting and the use and disclosure of credit sensitive information. Part IIIA of the Privacy Act governs the last two areas which are of particular interest today. Generally speaking, this Part of the Privacy Act only regulates consumer credit information – that is, information relating to a "loan" to an individual to be used wholly or primarily for domestic, family or household purposes. A "loan" is broadly defined in section 6(1) to cover, in effect, any debt deferral arrangement.

Broadly Part IIIA, as far as it relates to credit providers, regulates:

---

21 Section 51(2).

22 Section 163(1).

23 "Confidences – Bankers and Customers: Powers of Banks to maintain Secrecy and Confidentiality" Walter and Erlich, *The Australian Law Journal*, Volume 63, June 1989 page 419.

- the accuracy and security of credit reports (section 18G);
- access to, and alteration of, credit reports held by credit providers (sections 18H and 18J);
- the purpose for which credit providers can use credit reports (section 18L);
- the information which must be provided to an applicant where a credit application is refused wholly or partly on the grounds of a credit report in relation to the applicant (section 18M); and
- disclosure by credit providers of a "report" or personal information derived from a "report" (section 18N).

The restrictions in the Privacy Act on disclosure of a "report" or personal information derived from a "report" are of particular interest. In summary, section 18N prohibits the disclosure of such information for any purpose unless one of the various specified exceptions applies.

A "report" is broadly defined to include:

- a "credit report"; and
- any other record or information, in any form, that has any bearing on an individual's credit worthiness, credit standing, credit history or credit capacity;

other than publicly available information (section 18N(9)).

A "credit report" is essentially a report obtained from a credit reporting agency, such as the Credit Reference Association of Australia.

The exceptions provided for in section 18N(1), in summary, relate to disclosures:

- to a credit reporting agency for specified purposes;
- with the specific written agreement of the individual to another credit provider for a particular purpose;
- to a guarantor of a loan for enforcement purposes;
- to a mortgage insurer for specified purposes;
- to a dispute resolution authority;
- to a Minister, department or authority in a State or Territory whose functions include the giving of mortgage credit, or the management or supervision of schemes or arrangements involving mortgage credit;
- to a supplier for the purpose of allowing the supplier to determine whether to accept payment by means of a credit card or an electronic transfer of funds;
- to potential assignees;
- to debt collectors;
- to persons who manage loans for the credit provider;
- to related corporations;
- where disclosure for the particular purpose is required or authorised by or under law;

- to the individual themselves or a person authorised in writing by the individual to seek access to the relevant report or information;
- to a person authorised to operate an account maintained by the person; and
- in a case where there has been a serious credit infringement and the disclosure is made to another credit provider or a law enforcement authority.

This explanation of the exceptions available in section 18N(1) is very much an abbreviated explanation of the relevant provisions which merit careful attention.

Credit Reporting Code of Conduct

The Privacy Act's rules applicable to credit providers must be read in conjunction with the Credit Reporting Code of Conduct (Credit Reporting Code) which has been issued by the Privacy Commissioner under section 18A of the Privacy Act. The Credit Reporting Code has statutory force by virtue of section 18B of the Privacy Act.

The Credit Reporting Code, like Part III of the Privacy Act, applies only to consumer credit information and supplements Part IIIA.

Among other things, the Credit Reporting Code requires credit providers (including banks) and credit reporting agencies:

- to deal promptly with individual requests for access and amendment of personal credit information;
- to ensure that only permitted and accurate information is included in an individual's credit information file;
- to keep adequate records in regard to any disclosure of personal credit information;
- to adopt specific procedures in settling credit reporting disputes; and
- to provide staff training on the requirements of the Privacy Act.

Credit Reporting Advice Summaries

Part IIIA must also be read in conjunction with the Credit Reporting Advice Summaries issued by the Privacy Commissioner. These advice summaries do not have force of law but nevertheless clarify the Privacy Commissioner's view of many of the ambiguities inherent in section 18N(1). By way of example, the Privacy Commissioner is apparently of the view that a disclosure by a credit provider to certain service providers (such as lawyers, accountants, auditors, consultants and mailing houses) in connection with the management of loans provided by the credit provider may be regarded as a permitted "use" of information rather than as a prohibited "disclosure" provided the credit provider maintains control of the information and there are appropriate confidentiality provisions.[24] Such explanations of section 18N(1) are useful but they do not have the force of law and consequently there must some uncertainty in relying on them.

---

[24] Paragraph 10.24 of the Credit Reporting Advice Summaries issued by the Privacy Commissioner.

INTER-RELATIONSHIP BETWEEN THE COMMON LAW AND THE PRIVACY ACT

Interaction between the Privacy Act and Tournier's case

Part IIIA bears on the banker's common law duty of confidentiality as established by *Tournier's* case.

As a preliminary point it is noted that the *Tournier* duty of confidentiality attaches at the commencement of the bank/customer relationship commensurate with its contractual nature and terminates when the bank/customer relationship comes to an end.

The Privacy Act, in contrast, does not depend on a contractual duty but operates with statutory force in relation to certain consumer credit personal information. It is not affected by the commencement or cessation of the banker customer relationship. Hence, the Privacy Act imposes obligations on credit providers, including, but not limited to, banks, in a wider set of circumstances than *Tournier* does.

Furthermore, the rule in *Tournier* applies in respect of information, such as account information, concerning the conduct by the bank of the customer's business, irrespective of its source and purpose of collection. Part IIIA regulates, however, credit providers in respect of all information that comes within the broad definition of a "report". This latter class of information is clearly broader than the class of information in respect of which the *Tournier* duty of confidentiality attaches.

Many other aspects of Part IIIA exceed the *Tournier* duty of bank confidentiality. For example, the obligations concerning the collection of personal information, accuracy and security safeguards, restrictions on internal use of credit reports and permitted customer access do not clearly exist at common law. In contrast, the *Tournier* duty is confined to disclosure (and, to some degree, use).

The common law duty of non-disclosure also differs, however, from its counterpart provisions in Part IIIA. The best way to specify the differences is to examine the impact of Part IIIA upon the four exceptions to the common law rules.

Disclosure under Compulsion of Law and the Privacy Act

Privacy Act provisions

Under Part IIIA, the disclosure of a credit report by a credit provider is permitted if it is "required or authorised by or under law".[25] "Required" connotes compulsion such as mandatory legislation[26] or court order. A notable example of mandatory legislation is the Financial Transactions Report Act 1988 (Cth) which requires "cash dealers", inter alia, to supply reports of any transactions that they suspect on reasonable grounds may be relevant to the investigation of a tax evasion or a Federal offence.

"Authorised" indicates a right or entitlement, such as the right to disclose information under the Proceeds of Crimes Act 1987 (Cth) (for example, the right under section 46 of that Act to adduce evidence in relation to a proposed restraining order on property where the person appearing has

---

25 Privacy Act section 18N(1)(g).

26 For example, the Income Tax Assessment Act 1936 (Cth) sections 263, 264 (power to inspect and seize documents and to require disclosure of income and assets for use as evidence).

an interest in the property). The "compulsion of law" exception to the *Tournier* duty of confidentiality would not appear to be so broad as to allow disclosure on this basis.

The Credit Reporting Code contains the following explanation by the Privacy Commissioner of this exception which indicates it should be broadly interpreted and, in particular, that it should cover any disclosure allowed by *Tournier* (except to the extent that one of the other specific exceptions in section 18N indicates to the contrary):

> *"... where the disclosure is required or authorised by or under law. This applies to both statute law and common law. It is not limited to Commonwealth law but applies also to state law, and laws of other Australian jurisdictions to which credit providers may be subject. It also includes statutory provisions authorising warrants and other instruments for searching premises, obtaining information etc."*[27] (our emphasis)

Foreign laws

It would seem clear from the abovementioned statement that the Privacy Commissioner would not regard an order of foreign court requiring the production of credit sensitive information to be permitted under the "required or authorised by or under law" exception. This is because the Credit Reporting Code refers to Commonwealth and State law (as well as common law). However, there is no mention of foreign law. This would appear to be consistent with the position at common law. Although there is no Australian decision of which I am aware on what amounts to compulsion of law in an international context, English and Hong Kong cases indicate that the compulsion of law exception under *Tournier* does not include an order directed by a foreign court requiring the production of documents.[28] The rationale for these decisions appears to be that each branch of the bank is treated as independent of its parent body and is accordingly subject to the orders of a court in the country in which it operates but not to the orders of a foreign court (even if such an order emanates from a country in which the bank's head office is situated).

It would accordingly appear to be the case that a bank which is sent an order of a foreign court to produce documents could rely on its common law duties of confidentiality or the Privacy Act to refuse the production of a document. There is, of course, the possibility that the foreign country may seek assistance for the production of evidence in a criminal matter under the Mutual Assistance in Criminal Matters Act 1987 (Cth) (Mutual Assistance Act). The Mutual Assistance Act provides for requests made by a foreign country to an Australian entity to be referred to the Attorney-General who may then make an order requiring assistance to be provided.[29]

A further possibility is that a disclosure pursuant to the order of a foreign court may be regarded as permissible on the basis that it is in the public interest that the disclosure be made. This could occur in civil or criminal proceedings. In the case of *In re: Norway's Application (Nos 1 & 2 HL (E))*,[30] the English High Court was the recipient of a letter of request from a Norwegian Court requesting the oral examination of two witnesses who were bank officers. The witnesses opposed the order that they should submit to such oral examination on the grounds that, if compelled to give evidence, they would be forced to break their duty of confidentiality as bankers. Lord Goff of Chiveley stated:[31]

---

27 Paragraph 74 of Explanatory Notes to Credit Reporting Code.

28 *FDC Co Ltd v Chase Manhattan Bank NA* [1990] 1 HKLR 277 and *Power Curber International Ltd v National Bank of Kuwait SAK* [1981] 1 WOR 1233.

29 For example, the Attorney-General may order that evidence be taken for the purposes of a criminal proceeding (section 13(1)) or that documents and other articles in Australia be produced for the purposes of criminal proceedings (section 13(1)).

30 [1989] 2 WLR 458.

31 With concurring judgments from the other four Lords.

> "It is accepted on both sides that the question of confidentiality can only be answered by the court undertaking a balancing exercise, weighing on the one hand public interest in preserving the confidentiality owed by the witnesses as bankers to their customers, and on the other hand public interest in the English courts assisting the Norwegian court in obtaining evidence in this country."[32]

Re State of Norway (Nos 1 & 2 HL (E))[33] dealt with a civil letter of request which is in contrast to a criminal request which would emanate, for example, from a United States Grand Jury proceeding. However, the balancing exercise which is undertaken by the court is relevant to both requests. The likely effect of the request being criminal is that the court may give more weight to the public's interest in the administration of justice over the protection of the private right of confidentiality.[34]

Does the Privacy Act expand the Tournier compulsion of law exception?

The exceptions to the rule in *Tournier* differ somewhat from the circumstances where disclosure is authorised under Part IIIA. In some respects, Part IIIA expands the scope of disclosure by permitting disclosure on the basis that it is "authorised" by law (see first exception discussed above). The question is whether a disclosure "authorised" by law under section 18N is permissible in derogation from the common law duty not to disclose. Where there is an express intention on the part of the legislature to override the common law, this issue is not problematic. For example, the Privacy Act itself expressly allows disclosures between related corporations.[35] Such a disclosure would accordingly seem to be "authorised by or under law" and hence be within the section 18N(1)(g) exception and be permissible notwithstanding that it is not clearly within one of the exceptions to *Tournier*.[36] Many statutes "authorise" (as opposed to "require") disclosure, however in vague terms. In such instances, it is still arguable that Part IIIA will still authorise disclosure on the basis of the section 18N(1)(g) exception.

In other respects, disclosure under Part IIIA is more limited. This is almost certainly the case in relation to the giving of bankers' opinions.

Disclosure in the Public Interest and the Privacy Act

Part IIIA does not contain a general public interest exception to its disclosure rules although it does permit disclosure in circumstances where, on reasonable grounds, a credit provider believes that an individual has committed a serious credit infringement. A "serious credit infringement" is defined in section 6(1) of the Privacy Act to mean:

> "an act done by a person:
>
> (a) that involves fraudulently obtaining credit, or attempting fraudulently to obtain credit; or
>
> (b) that involves fraudulently evading the person's obligations in relation to credit, or attempting fraudulently to evade those obligations; or

---

32 *In re: Norway's Application (Nos 1 & 2 HL (E))* [1989] 2 WLR 458 at 479.

33 [1989] 2 WLR 458.

34 See also decision of Leggatt J in *XAG and Ors v A bank* [1983] 2 All ER in relation to foreign banks complying with Grand Jury subpoenas, in particular his comments in relation to the confidentiality of information given to Grand Jury proceedings at page 471.

35 Section 18N(1)(d) Privacy Act.

36 See *Bank of Tokyo Ltd v Karoon* [1987] 1 AC 45.

(c) that a reasonable person would consider indicates an intention, on the part of the first-mentioned person, no longer to comply with the first-mentioned person's obligations in relation to credit."

In such a case, information may be passed on to another credit provider or to a law enforcement agency.[37]

Disclosure in the Interest of the Bank and the Privacy Act

The counterpart of this exception in Part IIIA is narrower. Part IIIA permits disclosure to a person recognised and accepted in the community as being appointed for the purpose of settling disputes between credit providers and customers, for the purpose of settling such a dispute.[38]

Disclosure by Consent and the Privacy Act

At common law, there is scope for implying consent in certain circumstances. As far as individual consent goes Part IIIA should probably be regarded, however, as recognising only express consent to disclosure.[39] In particular, Part IIIA affects the giving of "bankers' opinions".

Part IIIA requires the specific consent of the individual to be given before a credit report or information may be disclosed by one credit provider to another.[40] This clearly covers the giving of a banker's opinion. It could be argued that, if at common law banks do have the implied consent of their customers to give opinions (which in itself may be debated), then the practice of giving opinions is "authorised" by law.[41] On this view, it should not be necessary to rely on the section 18N(1)(b) exception. Instead reliance might be placed on the section 18N(1)(g) exception for disclosures which are "authorised" by law.

On a purposive interpretative approach, it would, however, be anomalous to regard Part IIIA otherwise than as being intended to prevent the giving of bankers' opinions without consent. This is so notwithstanding the wide view expressed by the Privacy Commissioner as to what "authorised" by law means.

The position is, in any event, made clear by the Credit Reporting Code which provides that "a credit provider which is a bank may not disclose to another bank a 'banker's opinion' relating to an individual's consumer credit worthiness unless that individual's specific agreement to the disclosure of such information for the particular purpose has been obtained".[42]

STATE LEGISLATION

Privacy Committee Act 1975 (New South Wales)

The Privacy Committee Act established the Privacy Committee.

The Privacy Committee has broad investigative powers. It may, for example:

---

37 Section 18N Privacy Act.

38 Section 18N(1) Privacy Act.

39 Section 18N(1)(b) Privacy Act.

40 Section 18N(1)(b) Privacy Act.

41 Section 18N(1)(g) Privacy Act.

42 Credit Reporting Code 2.16.

- make reports and recommendations to any person in relation to any matter that concerns the need for or the desirability of action by that person in the interests of the privacy of persons;

- receive and investigate complaints about alleged violations of the privacy of persons and make reports to complainants; and

- conduct such inquiries and make such investigations as it thinks fit.

However, the Privacy Committee lacks any enforcement powers. It is obliged to report to the responsible Minister of its activities every 12 months.

Invasion of Privacy Act 1971 (Queensland)

The Invasion of Privacy Act deals with a number of issues relating to privacy, including credit reporting, listening devices and unlawful entry into a person's home.

As far as the credit reporting aspect of the legislation is concerned, the Act is limited in scope to consumer credit (credit to be used wholly or primarily for personal, family or household purposes). In that context, the legislation deals with the following issues (amongst others):

- there is a requirement for a credit report (which could include a banker's opinion) to be only provided on the written instructions of the consumer or to a person in connection with a credit transaction involving the person, an employer of the person or a related corporation of the person or the employer and the consumer on whom the report is furnished;[43]

- the notification by a user of a credit report to an individual of the refusal of credit and the individual's subsequent right to obtain access to information held by the credit reporting agent and his or her right to dispute the accuracy of that information;[44]

- the disclosure of credit reports (there is an offence for an unauthorised disclosure);[45] and

- deletion of stale information.[46]

Where a credit provider uses a credit report, then this legislation may apply. Were a bank to issue a banker's opinion in respect of consumer credit then it arguably could be caught as a credit reporting agent for the purposes of this legislation.

Fair Trading Act 1987 (South Australia)

Part V of the Fair Trading Act, which deals with fair reporting, is broad in scope and is not confined to credit.

Part V of the legislation applies to any communication made to a trader by a reporting agent or another trader of any information relating to a person, except where the person concerned is aware of the communication and the information. Such a communication is a "prescribed report".

A reporting agency is generally defined in the Act to mean a person that carries on the business of providing prescribed reports. A trader is a person, who in the course of a business, supplies, or

---

43 Section 16.

44 Sections 17 and 18.

45 Section 20.

46 Section 24.

offers to supply, goods or services. It is arguable that the provision of credit constitutes the supply of services.

The legislation requires a trader to notify an individual of certain information, including the name and address of a relevant reporting agency, where the trader:

- denies a prescribed benefit sought by the individual or grants a prescribed benefit sought by the individual on less favourable terms compared with other persons to whom the trader has granted prescribed benefits; and

- has obtained a prescribed report on the individual in the last 6 months.

A prescribed benefit includes a benefit of a commercial nature.

The legislation also deals with a person's right to gain access to information held by a reporting agency and a person's right to dispute the accuracy of the information.

The legislation may apply where a credit provider uses a prescribed report in respect of commercial credit. However, where a bank issues a banker's opinion (in respect of consumer or commercial credit), then it arguably could be caught by the legislation as a reporting agency.

Credit Reporting Act 1978 (Victoria)

As its name suggests, the Credit Reporting Act only deals with credit reporting. However, it is not limited to consumer credit. It applies to commercial and consumer credit and may apply to companies as well as individuals, despite its apparent restriction to "consumers". That is because a "consumer" is simply defined as "any person with respect to whom a credit report is made or with respect to whom any information is held by a credit reporting agent".[47] A "credit report" is in turn broadly defined in section 2. In particular, there is no "consumer purposes" test. Instead, the definition reads: "'credit report' means any written, oral, or other communication with respect to the credit worthiness, credit standing, or credit capacity of a person but does not include a report containing information solely as to transactions or experiences between the person making the report and the person who is the subject of the report."

The legislation primarily deals with the notification by a user of a credit report to an individual of the refusal of credit and the individual's subsequent rights to obtain access to information held by the relevant "credit reporting agent" (ie. essentially a person who engages in the practice of providing credit reports)[48] and to dispute the accuracy of that information.

A "credit reporting agent" has the following further obligations (amongst others):

- to give an affected consumer access to information compiled by the agent and the right to request corrections;[49] and

- to advise an affected consumer where amendments are made to relevant credit information and the obligation to advise any or all persons who have been supplied with information concerning the consumer in the previous six months and any other person requested by the consumer.[50]

---

47 Section 2.

48 See section (2) definitions.

49 Sections 5, 6(1) and 6(2).

50 Section 6(3).

Further State Privacy Legislation

There is the possibility of further State privacy legislation given the Prime Minister's announcement of 21 March 1997 that the Commonwealth Government would not be proceeding with its previously announced plans to extend the application of the Privacy Act to the private sector and given the privacy concerns that have been expressed by the States. As an alternative the Prime Minister appeared to envisage that business might develop voluntary codes with the assistance of the Privacy Commissioner.

In his press release the Prime Minister also said that he had asked the States not to enact their own privacy legislation and Queensland and the Northern Territory had agreed to that request. The position with other States, as at 15 May 1997, appears to be as follows:

- **New South Wales** – recent press reports suggest that New South Wales may introduce binding privacy rules for the New South Wales private sector.[51] However it is not expected that legislation will be released until the spring sittings of Parliament (at the earliest).

- **Victoria** – the Data Protection Advisory Council has prepared a report for the Government on privacy issues. The report has not yet been released pending preparation of the Government's response (it is not expected to be available until the spring session of Parliament at the earliest). However it is understood that the Council has recommended a State based privacy statute which regulates the public sector and has recommended that a private sector regime should be achieved with "maximum national uniformity". However it is not quite clear what the latter point means, especially in the context of the Prime Minister's announcement.

- **Tasmania** – is expected to release a privacy discussion paper in the week beginning 19 May 1997.

- **Western Australia** – a privacy working party has been established by the Government's Information Policy Committee to develop a best practice set of Information Privacy Principles and Guidelines. However it is understood that there is no intention to introduce legislation now or in the future.

INTER-RELATIONSHIP BETWEEN THE PRIVACY ACT AND STATE LEGISLATION

Section 3 of the Privacy Act provides that the Privacy Act is not to affect the operation of a State or Territory law that "makes provision with respect to interferences with the privacy of persons (including such a law relating to credit reporting or the use of information held in connection with credit reporting) and is capable of operating concurrently with this Act".

The Commonwealth therefore does not purport to cover the field in relation to credit reporting.

Accordingly, if there is no inconsistency with the Commonwealth Act, the relevant provision of the State law should be complied with whereas, if there is an inconsistency, the Privacy Act prevails.

---

51 See report in *The Australian Financial Review* on 18 April 1997.

INDUSTRY CODES

Electronic Funds Transfer Code of Conduct

The Electronic Funds Transfer Code of Conduct (EFT Code) is limited in application, applying to transactions intended to be initiated by an individual through an electronic terminal by the combined use of an EFT plastic card and a personal identification number (PIN).

Condition 10 of the EFT Code sets out the following privacy principles which a card issuer should follow in respect of EFT services they offer:

- customer records are to be treated in the strictest confidence;
- only the following persons are to have access through an electronic terminal to information about a customer's account:
  - an employee or agent of the financial institution who holds the customer's account;
  - the customer;
  - any person authorised by the customer;
- information about a customer's account can only be accessed through an electronic terminal where the request for the information is preceded by the entry of the correct card and PIN combination for that account (access by an employee or agent of the financial institution who holds the customer's account is excepted);
- information about a customer's use of EFT services is not to be disclosed by any financial institution unless it is provided:
  - pursuant to a legal duty or responsibility; or
  - with the customer's consent.

Condition 10 also provides that, where a camera may be used at an automatic teller machine to monitor transactions, card issuers are to display a sign indicating that transactions conducted at the machine may be photographed.

Code of Banking Practice, Credit Union Code of Practice and Building Society Code of Practice

The confidentiality provisions of the Code of Banking Practice (CBP) and the Credit Union Code of Practice (CUCP) are substantially to the same effect in that they both restate the *Tournier* rule with some slight modifications. The Building Society Code of Practice (BSCP) provisions concerning confidentiality are different in that there is simply stated a requirement to take "reasonable steps to maintain the confidentiality of a Customer's account details". There are exceptions for the situation where a customer has impliedly or expressly consented to the disclosure or the building society is compelled or authorised under law to disclose account details. There is no exception for disclosure on the basis that there is a duty to the public to disclose or that the interests of the building society require disclosure.[52] However, the exceptions relating to disclosures to related bodies corporate which exist in the CBP and the CUCP are contained in the BSCP.

---

52 See section 11.1 of the BSCP.

Perhaps of more interest are the substantive requirements of the CBP (which, as mentioned above, are also contained in the CUCP).

Under the CBP, a bank acknowledges its duty of confidentiality to a customer.

The following exceptions to the general duty of confidentiality are provided for under 12.1 and 12.2 of the CBP:

- the same exceptions as outlined in *Tournier* above;
- disclosure to another person with a customer's consent;
- disclosure to a related entity (as defined in the Corporations Law) for the purpose of assessing present and prospective liabilities of the customer to the bank and the related entity; and
- disclosure to a related entity which provides ancillary or related financial services to the bank unless the customer instructs the bank not to do so.

Under the CBP, a bank is also obliged to take reasonable steps to protect personal information held by it relating to a customer against loss or unauthorised access, use, modification or disclosure and require all staff dealing with personal customer information to maintain confidentiality concerning that information (12.10 CBP).

The remaining provisions of the CBP (12.3 – 12.9 CBP) deal with:

- the collection of information about a customer by a bank; and
- access to, and correction of, information about a customer by the customer.

ELECTRONIC BANKING AND PRIVACY ISSUES

Different Forms of Electronic Banking

There are a number of different forms of electronic banking which are becoming increasingly available. They include smart cards, digital cash, credit card transactions over the Internet, EFTPOS transactions and the use of automatic teller machines.

This fact was recognised in the Final Report of the Wallis Inquiry which provides that "Global retail electronic financial transactions are likely to emerge in the near future and will almost certainly flourish over the period to 2010 if the regulatory environment is accommodating". The Treasurer has also been reported as saying that regulation of electronic commerce is the biggest single issue arising from the Inquiry's report.

Electronic banking clearly brings with it an increased risk to privacy. These forms of commerce create extensive data documenting a transaction that can easily be stored, retrieved, analysed and reused. Most significantly, this data will be held on a public network with all the potential for access by third parties. Only a small amount of this data might have existed if cash had been used. I turn to consider some of the significant types of information that might be held in this electronic environment and in particular, the privacy issues that are created.

Smart Cards

A particular type of smart card, relevant in the electronic banking context, is the stored value card (or "electronic purse") (SVC). An SVC is an advanced version of a pre-paid card, which are widely used in Australia – for example, phone cards and pre-paid library photocopy cards. An

SVC is a plastic card which contains a micro-processor chip. The chip can store enormous quantities of information and perform simple computing operations.

The chip allows a consumer to store monetary value on the plastic card to be used later to purchase goods and services of any value. SVCs are designed to effectively replace cash in a wide variety of transactions ranging from the price of a telephone call, to public transport tickets, to everyday shopping. The value of the card is decremented as it is used until there is no residual value left and the card is then either recharged or thrown away.

SVCs have different design features and accordingly raise different privacy issues. An "accounted" SVC, for example, raises considerable privacy issues because transaction details can be recorded:

- on the card – which can be read by merchant terminals or the card issuer when the card is recharged, so as to provide information about the purchasing habits of the consumer;
- at merchant terminals – which can record details of the types of purchases made and the card number; and
- in a central data bank – where details of all transactions made with a card can be stored in a databank.

At the extreme end of the privacy concerns about a stored value card is a concern that they could be used to:

- track the movements of individuals (for example, they might be used to identify exactly the time and date of a purchase and where it takes place);
- identify the spending patterns of individuals (what they purchase and for how much); and
- identify "unusual" activity in the above areas.

These outcomes might be achieved by issuers developing systems which record data tracking transactions involving use of a card. Such information can be automatically generated in an electronic form and thus be cheap to store and process.

Internet

Current use of the Internet by credit providers

The Internet is widely used for electronic banking purposes at present.

Many credit providers have included financial services information on the Internet. Advance Bank and Commonwealth Bank of Australia also provide interactive services to its customers, including an ability to access account information, pay bills, transfer funds and order statements and cheque books. Advance Bank is also providing digital cash on the Internet. Others, including non-financial institutions, are bound to follow shortly.

There is also widespread use of credit cards to make purchases on the Internet.

Digital cash

Digital cash is a form of payment by electronic message on the Internet. It involves an issuer sending a digitally signed electronic message (known as a "digital coin") to a customer. The customer can store the digital coin on their computer and then use it to make a purchase by sending it to the merchant from whom the goods or services are ordered. The issuer would confirm that this digital coin had not previously been spent before the purchase was finalised and

then credit the merchant with the relevant amount. At each stage, there is a process of encoding and decoding the digital coin for security and verification purposes.

The privacy concerns here relate to information on any and all of the following subjects:

- the amount of digital cash purchased initially;
- the method that was used to pay for the digital cash;
- the identity of the purchaser;
- transaction details each time the digital cash is used;
- the balance of the digital cash account etc.

Credit card transactions

An added dimension in this context is concern about use of a credit card number to make a purchase on the Internet. You may well say that this concern should be exactly the same as a concern about disclosing a credit card number in a telephone purchase transaction. However, I would say the difference here is that the credit card details are being disclosed over a public network, ie the Internet. In this context, many security professionals might say that fears about sending credit card details over the Internet are misplaced because of the encryption devices which are becoming available. For example, the new security standards being developed by MasterCard, Visa, IBM, Microsoft and Netscape may help eliminate fraud.

Clearly the lower the security risks involved in using credit cards in the Internet, the lower the risk of privacy breaches.

Cookies

So what is a cookie? No, it is not something that you eat!

Anyone involved in an electronic banking transaction may receive a "cookie". Essentially they are a mechanism that allows simple data to be stored on a user's hard drive, thereby saving the storage space of the holder of the relevant Web site.

It is important to note that a cookie may be delivered by a server without the knowledge of the user.

In most cases cookies are helpful tools. For example, I fill out a Web site holder form with my name, address and other information. Perhaps a password. Cookies may be used to store this information so that the next time I visit the site the information is automatically uploaded and I do not have to provide it again.

The privacy implications of cookies relate to issues such as whether:

- sensitive information is encrypted on a cookie;
- they can be read or altered by third parties or by the Web Site that originally loaded the cookie on to your hard drive;
- they can read information from a user's hard drive which is then available to those with access to them;
- a user can have cookies placed on their system available for review without any knowledge that that is the case.

Electronic Banking – Key Privacy Concerns

There is no doubt that electronic banking raises a number of privacy concerns. It may be argued that these concerns are not valid and that they will exist regardless of whether a particular transaction involved any form of electronic communication. Nevertheless the concerns are there. Smart cards have been described by the New South Wales Privacy Commission as "Big Brother's little helpers". Privacy is also regarded as an extreme concern at an international level.

Some attempt has been made to deal with those concerns by the draft Internet Industry Code of Practice. This Code, prepared by the Internet Industry Association of Australia (INTIAA), focuses on the regulation of the Internet. It is intended to be binding on all members of INTIAA and on members of the industry who register under the Code.

There are a number of sections in the Code which impact on privacy matters. In particular:

- section 8 – secrecy obligations: contains obligations of confidentiality and restrictions on the sale or exchange of information;
- section 9 – data collection and use: regulates the collection and use of data relating to a user.

Those sections mean that organisations which agree to comply with the Code must:

- keep confidential the business records and personal information relating to their customers;
- take adequate steps to ensure the confidentiality of business records and personal information;
- not sell or exchange the business records or personal information of their customers other than to another organisation that has agreed to be bound by the Code or as part of the sale of the organisation's business as a going concern; and
- the Code expressly states that the above requirements do not prevent the disclosure of information with the express or implied consent of the customer or as required by law.

In relation to data collection and use, the Code describes the following principles:

- organisations will collect data relating to their customers only if it is relevant for the provision of the service that the organisation is providing to the customer, or for any other legitimate purpose made known to the customer prior to the time the data is collected;
- organisations can only use collected customer data for their own marketing, billing and other purposes necessary for the provision of the service they provide, or for other purposes only with the consent of the customer; and
- organisations must also ensure that the customer data they collect is accurate, up-to-date and if inaccurate is erased or corrected.[53]

The Warren Centre, Department of Industry, Science and Technology and the Asia-Pacific Smart Card Forum released in December 1996 a final draft of its Smart Card Industry Code of Conduct (APSC Code).

---

[53] See the discussion on the Internet Industry Code of Practice in the paper entitled "Privacy of Direct Marketing" presented by Mallesons Stephen Jaques practitioners Andrea Beatty and Katherine Forrest at the Business Law Education Seminar "Credit Code Update" held in Sydney on 24 April 1997 and in Melbourne on 30 April 1997.

The APSC Code contains a number of provisions dealing with privacy issues associated with smart cards including the following:

- the purposes for which personal information is collected and to whom it may be disclosed must be explicit and disclosed to the cardholder before collection (any variation to the relevant purpose must also be advised to the cardholder who must then be given the opportunity to consent);
- the cardholder must have the opportunity to refuse consent to a particular use of personal information beyond the immediate purpose for which the information was obtained or any proposed new purpose;
- personal information must be accurate and kept complete and current (where that is necessary for the purposes of processing);
- personal information may be disclosed to a person who delivers services to the cardholder in association with the entity bound by the APSC Code if the purpose of disclosure has been advised to the cardholder who has not objected; and
- it is permissible to make a use or disclosure which is compelled by law, to which the cardholder has consented or which is made in an emergency to protect life or prevent injury or serious damage to property.

Inter-relationship between Electronic Banking and the Privacy Act

Part IIIA does not readily apply to electronic banking. This is best evidenced by the legal issue to do with the Privacy Act's "in writing" requirement.

As mentioned above the Privacy Act prohibits the disclosure of a "report" or any personal information derived from a report that is, or has been, in the possession of a credit provider to another person for any purpose (section 18N(1)).

There are several exceptions to the general rule, including permitting the disclosure of personal information to another credit provider for a particular purpose where the individual concerned has specifically agreed to such disclosure (section 18N(1)(b)). The agreement must be "in writing" unless the disclosure is sought for the purpose of assessing an application for consumer or commercial credit that was initially made orally and the application has not yet been made in writing (section 18N(1A)).

The Privacy Act does not define "writing". However, section 25 of the Acts Interpretation Act 1901 (Commonwealth) provides that:

> "In any Act, unless the contrary intention appears .... 'writing' includes any mode of representing or reproducing words, figures, drawings or symbols **in a visible form**".

The critical issue is whether an electronic message on the Internet falls within the scope of the words "in a visible form" and therefore constitutes a "writing". A literal interpretation of this definition of writing would preclude electronic messages, and thereby, Privacy Act consents could not be given over the Internet.

It may be that some organisations will be prepared to take a bullish view of the "in writing" requirement. However, credit providers render themselves liable to a maximum fine of $150,000 if a court determines that a consent given via the Internet is not "in writing" and as such the credit provider has recklessly or knowingly contravened the Act.

EUROPEAN UNION DIRECTIVE AND ITS IMPACT ON AUSTRALIAN BUSINESS

The European Directive

Privacy is a concern at an international level. This concern is evidenced by the terms of the requirements of the European Directive entitled "Directive on the Protection of Individuals With Regard to the Processing of Personal Data And on Free Movement of Such Data" (European Directive). The European Directive is due for adoption by Member States by October 1998.

The European Directive's stated objective is to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data. The Directive is intended to apply equally to public and private sector organisations.

This part of the paper considers:

- the terms of the European Directive and, in particular, the restrictions on transborder data flows; and
- how the Directive may impact Australian businesses.

Privacy Principles

The Directive sets out a number of principles relating to, among other things:

- data quality – requiring the collection of personal data for specified and legitimate purposes, keeping personal data accurate and up-to-date and retaining personal data for no longer than necessary (article 6);
- data processing – which involves permitting data processing only in certain circumstances, including where the data subject has given consent, where the processing is necessary to protect the data subject, or where the processing is in the public interest (article 7);
- special types of data – prohibiting the processing of personal data about racial or ethnic origins, political opinions, religious or philosophical beliefs, trade-union membership, health and sex life except in certain circumstances (article 8);
- information disclosure to a data subject – requiring the provision of certain information to a data subject where data relating to them is collected, including the purpose for which data is collected (articles 10 and 11);
- access to data – which deals with a data subject's right to access personal data and other information and with the right to rectify incorrect information (article 12);
- confidentiality and security of processing – which involves the implementation of technical and organisational measures to protect data (articles 16 and 17); and
- transfer of personal data to third countries (article 25). In summary article 25 requires Member States to provide that the transfer to another country of personal data for processing can only take place if the country in question ensures "an adequate level of protection". The adequacy of the level of protection of a country is to be assessed in light of all the circumstances surrounding a data transfer operation or set of data transfer operations, including the nature of the data, the purpose and duration of the processing operation and the professional rules and security measures which are complied with in the third country (article 25).

"Processing of personal data" is defined broadly to mean "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction".

Privacy Principle dealing with Transfer of Personal Data to a Third Country

The last principle mentioned above may, for example, be of particular concern to Australian banks who:

- have branches or subsidiaries or a head office in Europe and wish to transfer data to Australia; or
- wish to use data processing facilities in Europe and wish to transfer data to and from Europe for that purpose (the data processing might, for example, cover statement preparation, risk modelling or credit assessments).

The concern is the lack of wide ranging privacy legislation applying to the private sector in Australia may result in Australia's isolation from international data flows. Whether this concern is real remains to be seen.

It might be, for example, that Australian banks already have an adequate level of privacy protection even without any new legislation given:

- the *Tournier* duty of confidentiality implied into contracts;
- the equitable duty of confidentiality and the rules applicable to fiduciary relationships; and
- the Code of Banking Practice (on the basis that professional rules may be considered when determining whether a country has an adequate level of privacy protection).

There are also a number of exceptions to the European Directive's restrictions which may be relevant. For example, there are exceptions:

- where the individual concerned has consented "unambiguously" to the transfer of data (the definition of "the data subject's consent" in article 2(h) states that this expression "shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed");
- where the transfer is required by a contractual (or pre-contractual) arrangement with the data subject;
- where the transfer is necessary to perform a contract concluded in the interests of the data subject;
- where the transfer is necessary on public interest grounds for the purposes of legal claims or to protect the "vital interests" of the data subject;
- where the transfer is from a public register (provided any consultation conditions are met); or
- where a Minister has authorised the transfer on the basis of guarantees by the data controller designed to protect the privacy and fundamental rights and freedoms of the individual concerned (it is contemplated that the guarantees could be provided by appropriate contractual clauses).

The Impact the Directive may have on Australian Business

Government response to Directive

As stated above, on 21 March 1997 the Prime Minister announced that it would not be implementing privacy legislation for the private sector. The Prime Minister also announced that he has asked the Premiers and Chief Ministers of each State and Territory not to introduce legislation on this matter within their own jurisdiction. At the time of writing only the Northern Territory and Queensland Governments have agreed not to introduce such legislation. However New South Wales seems likely to introduce such legislation and the position in the other States is not yet certain (see the section entitled "Further State Privacy Legislation" above).

Privacy Commissioner's response to Directive

The Commonwealth Privacy Commissioner, Ms Moira Scollay has been reported[54] to have announced that she would be developing a voluntary national privacy code which would be capable of meeting the standards of the European Union and could be backed by legislation from any Australian Parliament at a later stage. It appears that the voluntary code will be based on the Canadian code model.

Consumers' response

An international group called Privacy International has said that it will push for the European Union to impose economic sanctions against those third countries which do not ensure adequate privacy protection.

Australia is a likely target. Privacy International's Director-General, Simon Davies, has stated that a bank, the banking sector as a whole or the airline sector are likely to be the particular targets of any action for economic sanctions.

However, it is questionable whether any action against a bank or the banking sector would succeed. As mentioned above, it is arguable that there are in fact adequate levels of privacy protection in Australia.

WALLIS INQUIRY'S RESPONSE TO PRIVACY ISSUES

It is important to note in this context that the Final Report of the Wallis inquiry was submitted to the Treasurer, Mr Peter Costello, on 18 March 1997 – that is, before the announcement by the Prime Minister not to proceed with the implementation of privacy legislation in respect of the private sector.

The Inquiry recommends that:

- significant legislative change be made to facilitate electronic commerce which does not differ depending on the technology or delivery mechanisms used (the Inquiry earmarked certain Acts in particular, including the Privacy Act);

- privacy legislation be reviewed and privacy codes developed on a functional (rather than instrumental) basis, to apply to all who supply financial services;

---

[54] See article in *The Australian Financial Review* on 18 April 1997 entitled "Privacy chief to take hands-on role".

- information sharing among group entities should be allowed unless a customer has taken some action to indicate that they refuse their consent (if this recommendation were implemented it would help overcome a significant practical difficulty currently faced by members of a financial conglomerate on information sharing); and

- the Commonwealth Attorney-General should establish a working party to review existing credit provisions of the Privacy Act 1988 with a view to identifying restrictions which prevent the adoption of world's best practice techniques for credit assessment which could include the current restrictions on positive credit reporting.

Recommendation 101 dealt with the issue concerning the extension of the current privacy regime in the following terms:

> "The approach to privacy regulation which emerges from the current consultative process should:
>
> - strike an appropriate balance between consumer protection, consumer choice and the effective and efficient delivery of financial services to consumers;
>
> - be carried out in a way which enables it to adapt to the changes accruing in the market, including convergence in financial service providers and products
>
> – this suggests that any laws or codes or practice should apply to the function of financial service provision rather than to financial institutions;
>
> - be administered for the financial system by the Privacy Commissioner on a national basis;
>
> - avoid or eliminate any duplication of coverage between existing privacy protection, including credit reporting provisions of the Privacy Act 1988 and financial sector codes of conduct, and the proposed privacy codes; and
>
> - ensure appropriate transitional arrangements are introduced for information which was obtained prior to the introduction of the proposed privacy regime."

CONCLUSION

There are essentially two drivers of change in privacy laws. First, the need for the Privacy Act to be brought into the electronic age so that it can have ready application to things like smart cards and the Internet. Secondly, the push for privacy protection for consumers dealing with the private sector.

It is submitted that the first driver of change is the real issue for credit providers. Furthermore, such a change could be made through generic legislation, which could amend several pieces of legislation at once, and not necessarily through a process of amending legislation in a piecemeal fashion. Ideally, any developments in this regard should also be co-ordinated at an international level. For example, any work on digital signatures should be done by reference to the work on digital signatures and certification authorities currently being undertaken by the UNCITRAL Working Group on Electronic Commerce.

It remains to be seen whether the second driver will be a real issue for credit providers. If the States pass dis-uniform privacy legislation then it will most certainly be an issue. It is also likely that the development of the different forms of electronic banking may increase the demand for more privacy protection. Whether the European Directive is also an incentive for change will be a matter of testing whether the members of the European Union consider that, for consumers of financial products at least, there is an adequate level of privacy protection. Failing that, the exceptions to the rule against transferring personal data to a third country can be tested. If the consumer lobby groups, such as Privacy International, are anything to go by, it seems that it will

not be long before the private sector, in particular banks, will be required to put this issue to the test.

The risk of new forms of privacy regulation begin developed might, of course, be reduced if Australian businesses are proactive in ensuring that their contracts contain adequate confidentiality provisions and that they have adopted privacy codes of practice which implement the objectives of the European Directive.

Whatever the outcome there is to the privacy issues dealt with today, let us hope that there is:

- uniformity and consistency across regulatory forms;
- co-ordination at an international level;
- a balancing of the interest of consumers and business;
- a recognition of the needs of convergent industries; and
- a recognition of the transitional issues associated with the information already held on individuals.