KATRINE ELISABETH SHARP

CHEQUES AND BALANCES

-

THE CODE OF BANKING PRACTICE AND DATA PRIVACY

Submitted for the LLB (Honours) Degree
at the Victoria University of Wellington

1 SEPTEMBER 1992

TABLE OF CONTENTS

INTRODUCTION

> Suppose that JB, aged 18, decides that the time has come to open a bank account. She goes to the Harbourside Savings Bank on Lambton Quay, and fills in the necessary forms giving her name, address, date of birth, contact telephone number, and so on. From now on, JB is the subject of a computer file at Harbourside and the basic information she gave to open the account will gradually be supplemented, and occasionally altered, according to her changing circumstances. She may acquire a full-time job, with her salary paid directly into her account, purchase a house with the assistance of the bank, start a company with a further loan from the bank, or apply for a credit card. Every detail of her dealings with the bank will be noted on her file.

None of this, nor indeed any of the rest of this paper, is aimed at engendering a "Big Brother Is Watching You" mentality. In order to operate successfully, banks must necessarily have the information with which to conduct accounts and on which to base decisions relating to their customers. However, the above example does show that banks can and do compile very significant amounts of data, financial and otherwise, about their clients. Banks are an essential and very sizeable cog in the machinery of the modern state, vital to individuals, to commerce and to the economy as a whole. What they do with the information at thir disposal can have very far-reaching effects.

In the past, measures to protect the privacy of customers have been strictly limited. Banks have usually given priority to their own interests, and the courts have allowed them to. In March of this year, however, the seventeen members of the New Zealand Bankers' Association adopted a new, voluntary, Code of Banking Practice, which contains provisions to protect customer information. These provisions

are fairly closely modelled on the Privacy of Information Bill, which was introduced into Parliament in 1991. The Bill sets out a number of 'Privacy Principles' [1] against which complaints about breaches of privacy are to be assessed by the Privacy Commissioner. It applies both to the private and the public sectors and seeks to provide much greater protection of personal data privacy than individuals have had up to now. The Bill has been referred back to select committee for further submissions, but it looks likely to be enacted within the next two or three years. Meanwhile, pre-empting the proposed legislation, the banks have changed their own emphasis considerably towards greater customer protection by adopting the basic principles into the Code of Practice.

This paper will examine the provisions in the Code of Banking Practice in the context of the general debate on privacy, and will assess their effect on previously accepted banking practice. It will also seek to assess whether the Code is adequate to protect bank customers' privacy, or whether legislative intervention in the shape of the Privacy of Information Bill is still desirable.

---

1 These are based on the Principles for National Application in the OECD Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Data (1980), and the Council of Europe's "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data"(1981).

I THE PRIVACY DEBATE

The first question to be asked is why the law should protect an individual's privacy at all. Tim McBride's paper on data privacy cites an argument that our interpersonal relationships are essentially based on respect for each others' privacy.[2] Perhaps for this reason, it has been accepted as a fundamental human right in Article 12 of the Universal Declaration of Human Rights 1948, in Article 17 of the International Covenant on Civil and Political Rights 1966 and, in the limited form of a right not to be subjected to unreasonable search and seizure, in section 21 of the New Zealand Bill of Rights Act 1990, among others.

However, the common law courts, with some exceptions in the United States, have been very reluctant to extend the present common law to protect a person's privacy per se. If a complaint cannot be brought under the mantle of such areas as defamation, trespass or breach of contract, then the complainant probably has no remedy at law.[3] It may in certain limited circumstances be possible to bring an action for breach of confidence under the court's equitable jurisdiction. Despite the considerable expansion of this field in recent years, however, it cannot be regarded as generally available for breaches of privacy.[4]

The reluctance of the courts is in many ways readily understandable. The general area of privacy is extremely wide and vague, damage is difficult to quantify in many

---

2 T. McBride Data Privacy : An Options Paper (Department of Justice, Wellington, 1987),13.

3 The closest that New Zealand courts appear to have come to accepting the limited protection of the tort of 'public disclosure of private facts' is in Tucker v News Media Ownership Ltd [1986] 2 NZLR, 735 per McGechan J.

4 McBride, as above note 2, 54-59.

cases, and an individual's "right to privacy" frequently clashes irreconcilably with other fundamental rights such as freedom of speech. Applying demarcation lines so as to allow some forms or degrees of breach of privacy to be actionable and not others is in many cases practically impossible. In 1975, Palmer pointed out the futility of questing after a general law on privacy, and recommended that specific measures be taken in areas where a need is clearly demonstrated.[5]

One of these areas is data privacy, a relatively small, though growingly important subset of the general field. Many jurisdictions throughout the world have enacted legislation to protect data subjects, among them the United Kingdom, the United States, Canada and Australia.[6] In fact, New Zealand is a noticeable exception to the general trend of enacting privacy legislation.

Data privacy can be defined as the interest of the individual in controlling the circulation of information personal to him or her which is held by others.[7] Personal information is information held about an identifiable person.[8] Protection of data privacy can clearly not be absolute, however, but must be balanced against competing public and private interests:[9]

> A balance must be found between the interests of the individual and the interests of society, which include the efficient conduct of industry, commerce and administration.

So, a requirement that banks should maintain total secrecy with regard to their customers' accounts would be

---

5 G. Palmer "Privacy and the Law", (1975) NZLJ, 747-748.

6 Data Protection Act 1984 (UK), Privacy Act 1974 (USA), Privacy Act 1982 (Canada) and Privacy Act 1988 (Aust).

7 McBride, as above note 2, 14.

8 Official Information Act 1982, s.2.

9 Report of the Committee on Data Protection (1978, Cmnd 7341) para 2.09.

unreasonable. The public interest in detecting crime, for example, entitles agencies such as the Serious Fraud Office to obtain access to customer records. Also, it would unduly restrict a bank's ability to function efficiently if it were unable to protect itself by producing customer information in litigation against that customer.

The growth in information technology, especially over the last decade, is the main reason for the rise in public concern about data privacy. Info-technology has now advanced to the point where it is possible to build very detailed profiles of data subjects using separate items of information from various sources. All customer transactions with a bank, for example, must be recorded and stored for seven years before destruction.[10] Add to this various items of publicly available information, and the network facilities available to banks enable them, or agencies which have access to their records, to compile a reasonably accurate picture of a person's life. This is not to say that such profile-building takes place regularly, but where the technological capability exists, so does the potential for abuse. The threat of 'hackers' gaining access to data storage systems, and the huge increase in transborder flows of personal data compound the problem further.[11]

Various international bodies are involved in attempts to regulate the area of data privacy, among them the Council of Europe and the Organisation for Economic Co-operation and Development. The latter, for instance, produced its "Guidelines on the Protection of Privacy"[12] in 1980 as a response to the growing public concern. Its main aim was to facilitate harmonisation of member countries' data privacy

---

10 Section 12, Banking Act 1982.

11 Thus the main threat to data privacy comes from automated data systems. It may be argued that the Privacy of Information Bill's coverage of manual as well as automated systems is overkill, but this is not examined in this paper.

12 As above, note 1.

laws. To achieve this, the Guidelines set out "Basic Principles of National Application".[13] This is a statement of what the drafters[14] considered to be minimum standards of data privacy to which member states should adhere.[15] Compliance with the principles by signatories should ensure both that the individual's right to data privacy is adequately protected and that the free flow of data between those signatories is enhanced, since equal protection of the information in the recipient country is guaranteed. New Zealand adopted the Guidelines on 23 September 1980, together with fifteen other member states.

The Guidelines are merely recommendatory in nature, and do not bind their signatories in international law. It was, however, envisaged that "[t]he Guidelines could serve as a starting point for the development of an international Convention when the need arises".[16] In the meantime, the Council of the OECD recommended that "Member countries take into account in their domestic legislation the principles ... set forth in the Guidelines".[17]

A summary of the privacy principles is as follows:

Collection

> Information should not be collected unnecessarily, and is to be obtained by lawful and fair means (ie. not obtained by coercion or deception). If financial or other pressures effectively mean consent to give information is compulsory (as with applying for a bank loan) the donee may be under a stricter obligation to observe the other protective measures.[18]

---

13 Part Two, paras 7-14.

14 An Expert Group, under the chairmanship of the Honourable Mr Justice Kirby of Australia.

15 Part One, para.6.

16 Explanatory Memorandum, page 24.

17 Recommendation of the Council, clause 1.

18 McBride, as note 2, 16.

The information should be relevant to the purposes for which it is collected, and should be as accurate, complete and up-to-date as is reasonable.

Storage

"Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data."[19]

Use and disclosure

An agency must not disclose, make available or use personal information for a purpose other than that for which it was obtained. Exceptions to this are limited, but include where the purpose for which the information is disclosed is directly related to the purpose for which it was obtained, or the disclosure is authorised by law.

Access

Individuals should have the right to be told by the agency whether data relating to them is or is not held by that agency. They should have access to the data within a reasonable time, at a charge, if any, which is not excessive. The information should be given in a form which they can easily understand.

If such a request is denied, the data subject should have the right to reasons for the denial, and the right to challenge the denial. If the information is inaccurate, incomplete or out-of-date, then the individual to whom it related should have the right to have it rectified or erased.

The Guidelines are one of the main motivating forces behind the New Zealand Government's introduction of the Privacy of Information Bill into Parliament. The principles set out in the Bill accord closely with the 'minimum standards' of the Guidelines. Originally, the Bill also contained provisions to allow information-matching programmes to combat welfare-

19 OECD Guidelines, as note 1, Part Two, para.11.

fraud.[20] For reasons of political expediency, given the even more contentious nature of the rest of the Bill, the Government decided to enact these provisions separately. The Privacy Commissioner's Act 1991 thus establishes the office of Privacy Commissioner as general overseer of privacy issues and as approver of information-matching programmes.[21] The main body of the Bill, however, remains before select committee. It contains the fourteen privacy principles, provisions dealing with good reasons for refusing access to personal information, and provisions for exemptions from the principles. It also gives details of the complaints procedure to be followed, and amends various other Acts such as the Official Information Act. The legislation is still far from trouble-free, but it is the writer's view that its unifying theme of data privacy protection makes it an improvement on the original.

One of the most contentious aspects of the Bill is its application to the private as well as the public sector. Agencies such as banks, which hold a great deal of personal information, are therefore one of its principal targets. The private sector has produced some highly vocal opponents of the Bill, among them the Direct Marketing Association.[22] It claims that the "draconian" provisions of the proposed legislation will have a disastrous effect on the access to databases which is at the heart of the direct marketing business. The principles in the Bill, it argues, do not achieve the correct balance between the individual's interests and the interests of commerce.[23] The Newspaper

---

20 One of the first programmes to be reported is that between Customs and Social Welfare, The Dominion, Wellington, 21 July 1992.

21 The Privacy Commissioner cannot therefore as yet receive complaints about breaches of data privacy.

22 Others include various charitable organisations and arts groups.

23 Memorandum to the Minister of Justice from the Department of Justice, 28 June 1991, annex.

Publishers' Association criticises the Bill as impinging too much on the freedom of the press to use and collect personal information. It also claims that the Bill takes "no account of the day-to-day running of a media organisation".[24] However, the writer contends that there are strong arguments in favour of the inclusion of the private sector in the legislation.

Firstly, the information about which people are most sensitive relates to income, assets and credit, which is information most commonly held by private sector organisations.[25] The Annual Report of the (Australian) Privacy Commissioner in 1989 said:[26]

> Many argue that there is more to be found by way of privacy invasion in the private sector. The argument runs that governments are publicly accountable for their actions and subject to the oversight of Parliament and their employees are subject to severe sanction for breaches of discipline or confidentiality ... These constraints do not apply in the private sector. Yet the private sector organisation often has incentives (profit) and resources to acquire new technology which far outstrip those of government.

Over ninety percent of businesses in New Zealand now have some form of database.[27] It therefore seems in many ways illogical to enact privacy legislation covering only the public sector, especially considering the protection already afforded by the Official Information Act.

---

24 Letters, The Listener, 6 April 1992.

25 Speech by The Hon. Douglas Graham, Minister of Justice, to the Criminal Bar Association AGM, 27 September 1991.

26 First Annual Report of the Privacy Commissioner, 1 January 1989 to 30 June 1989, page 45. This confidence in the public service may seem rather misplaced, however, in the light of revelations about the sale of personal information in government computers in Australia, The Dominion, Wellington 14 August 1992, 5.

27 As above, note 23.

Secondly, the OECD Guidelines apply both to the private and the public sectors. New Zealand should therefore follow that approach in implementing the Guidelines in domestic legislation. So far, twenty three out of twenty seven states with data privacy legislation cover both sectors.[28] It has been suggested that countries without adequate legislative provisions may be unable to participate to the full in the international information market. Application to the private sector is therefore essential if this threat is to be eliminated.

Thirdly, in other areas of law, for example administrative law, there has been a general blurring of the public/private distinction. It has been recognised that what matters more than the nature of the body is to what extent the actions of an agency have public effect. This is especially important as changes are made to the bureaucratic structure with formerly publicly-controlled assets being transferred into private hands through corporatisation and privatisation. The writer suggests that, in the same way, the emphasis in privacy law should not be on whether an agency is private or public sector. Rather, we should concentrate on the effect that data-collecting agencies of all kinds have on their data-subjects. Agencies such as banks, insurance companies and credit reference agencies have enormous public effect. Data subjects need adequate protection regardless of which agency holds the information.

The Government has recently indicated that the political will to tackle the privacy issue is alive and well. It therefore seems likely that the Bill, with its core of privacy principles, will be passed within the next few years. Meanwhile, organisations such as the banks have turned their minds to self-regulation. This may be partly an effort to postpone more stringent legislative intervention for as long as possible; there is certainly a good deal of mileage to be gained from producing an effective self-

---

28 Department of Justice, "The Information Privacy Bill - Application to the Private Sector", 28 March 1991.

policing scheme. Also, such organisations are very well aware of the increased public awareness of privacy issues,[29] and those with effective protective mechanisms may gain a competitive advantage in a tight market. This therefore, is the genesis of the new Code of Banking Practice, with its provisions for greater protection of customer information.

---

29 Elisabeth Longworth "Final Word", The Dominion, Wellington, March 30 1992, 20.

II THE PRESENT LEGAL POSITION

With the exception of some statutory provisions, which have no bearing on the privacy issue, the relationship between banks and their customers has hitherto been defined and governed by the common law. The only aspect of the relationship, as dealt with by the courts, which protects customer data privacy is the bank's duty of confidentiality. This is the duty not to disclose information relating to the customer which the bank obtains in the course of handling the customer's account. Thus, the other fundamental principles of data privacy, such as access and use limitation, have up to now had no place in banking law.

The Banker's Duty of Confidentiality

The law on the topic of disclosure is of fairly modern origin in banking terms. The leading case in the field is Tournier v National Provincial and Union Bank of England,[30] and it is recognised and applied equally in New Zealand.[31] Prior to this, it was uncertain whether the bank's duty of confidentiality was a legal, or merely a moral duty. Also, if it was a legal duty, it was unclear under what circumstances, if any, it might still be "reasonable and proper" to communicate information to a third party.[32] The Court of Appeal in Tournier, however, unanimously decided that the duty of the bank to keep its customers' affairs secret is a "legal one arising out of contract".[33] The scope of the duty was indicated by Atkin LJ:[34]

> It clearly goes beyond the state of the account, that is, whether there is a debit or a credit balance, and the amount of the balance. It must extend at least to all the transactions that go through the account, and

30 [1923] 1 KB 461.

31 See for example M. Russell Introduction to New Zealand Banking Law, 58; Tyree New Zealand Banking Law, 84.

32 Hardy v Veasey L.R. 3 Ex. 107.

33 Tournier, as note 30, per Bankes LJ at 472.

34 Tournier, as note 30, at 485.

> to the securities, if any, given in respect of the account; and in respect of such matters it must, I think, extend beyond the period when the account closed or ceases to be an active account ... I further think that the obligation extends to information obtained from other sources than the customer's actual account, if the occasion upon which the information was obtained arose out of the banking relations of the bank and its customer ...

The duty is, necessarily, not absolute, but qualified, and the accepted qualifications to it are those set out by Bankes LJ at page 473:

> a) where disclosure is under compulsion by law;
> b) where there is a duty to the public to disclose;
> c) where the interests of the bank require disclosure;
> d) where the disclosure is made by the express or implied consent of the customer.

a) Compulsion by law.

A growing number of statutes in New Zealand allow access to customer records by such agencies as the Inland Revenue and the Serious Fraud Office.[35] It is clear that banks must comply with the requirements of statute.

This exception also covers court orders, such as orders for discovery when a bank is a party to proceedings.

b) Duty to the public

This duty covers disclosures made in exceptional circumstances, for example to prevent death or injury to another, or in matters of national security or prevention of serious crime. These types of situations, however, are almost completely covered by statutory compulsion to

---

35 All statutes allowing access to customer records are listed in the Annex (II) to the Code of Banking Practice. Many thousands of inquiries are made each year.

disclose, so this exception may be largely unnecessary.[36]

c) The interests of the bank

The interests of the bank may clearly override confidentiality when a bank engages in litigation with a customer or with a guarantor. However, only information which is strictly relevant to the proceedings should be used.[37]

The two main areas of uncertainty are disclosures made within the banking group and disclosures to credit reference agencies. Banks may feel entitled to release information without customer consent to other companies within their banking group, some of which may be non-banking subsidiaries. This is of growing concern in New Zealand, as banking groups expand, and most customers are unaware of the identities of the various members of the groups. However, in Bank of Tokyo Ltd v Karoon,[38] it was said that each corporate entity within the banking group must be viewed as a separate entity for confidentiality purposes. Consent may therefore be required for disclosure. It is arguable, though, that passing information to such of the subsidiaries as are banks is cost-effective and acceptable, provided it is for a strictly defined purpose. Consent should be obtained prior to disclosure to non-banking subsidiaries.[39]

Credit reference agencies collect information on the creditworthiness of a person from public sources and from providers of credit who are willing to release information.

---

36 But see Libyan Arab Foreign Bank v Bankers Trust Co [1988] 1 LLR 259, where a higher duty to the public was tentatively accepted though other exceptions did not apply. R Grandison, in F. Neate, R. McCormick (eds) Bank Confidentiality (Butterworths, London, 1990),96.

37 As above, note 36, at 95.

38 [1987] AC 45.

39 Banking Services: Law and Practice. Report by the Review Committee (The Jack Report)(UK, December 1988).

They then sell the information to potential lenders. It appears that in the United Kingdom at least, banks have until recently made use of this information but have not themselves contributed. There is, however, a clear trend towards banks making more information available to such agencies, although this is not clearly covered by any of the Tournier exceptions.

d) Consent.

Clearly no problem arises if a customer expressly consents to the disclosure of information. However, implied consent is a contentious subject. Most bank customers are quite unaware of many of the terms of their contract with the bank, and so implying consent to disclosure under certain circumstances is fraught with difficulties. For example, it was supposedly an implied term that bankers' references could be given to third parties, yet few customers would have been aware that such practices existed.[40]

Another potential problem in this area is the recent development in the United States of issuing consent directives. These are documents in which a customer authorises a bank to release information about himself or herself to government authorities. The customer has been compelled to sign the documents by court order, under threat of fines or imprisonment. The status of such directives is uncertain, for it is fundamental that consent must be freely given. A bank's refusal to disclose information under a consent directive may mean that the customer is exposed to an action for contempt of court, however.[41] Such practices are as yet unknown in New Zealand, but conflicts will arise with the duty of confidentiality and with any privacy legislation if they are introduced here.

---

40 In practice, bankers' references have not been given without consent here for some time. Consent is now required by the Code of Banking Practice, para. 10.4.2.

41 Bank Confidentiality , as note 36, at 91-92.

Therefore, although on the face of it Tournier's case appears to provide fairly thorough protection for the bank customer, the above discussion illustrates some of the areas of difficulty and uncertainty, which seriously undermine the protection afforded.

The Code of Banking Practice

The new Code of Banking Practice was introduced on 1 March 1992. It aims to rectify some of the difficulties inherent in banking law, where bank/customer relations are based on a contract with mainly implied terms. This is done by setting out minimum standards of good banking practice, thus making the terms of the contract more "transparent". At the same time, competition should be stimulated by making it easier for consumers to compare services offered by the banks. The Code is a voluntary, industry-produced document, and customers will still make individual contracts with their banks. However, the Code should, it is suggested, be treated by the banks as if it were legally binding on them.

There are several reasons for this. Firstly:[42]

> it is impossible to say that the Code raises or sets minimum standards of fair dealing unless banks are committed to honouring it. And to the extent that the Code seeks to stifle any inchoate urge on the part of the Government to legislate, no bank will try to persuade a Court that non-compliance can be excused because the Code is legally meaningless.

Secondly, if comparison between the banks is facilitated by better informing the consumer as to minimum standards of practice, it would not make sense commercially to fall below those standards.

---

42 F. Miller "Code of Banking Practice - What Will It Mean For Banks?" (unpublished paper delivered to New Zealand Bankers' Association conference, 1991) at page 2.

Thirdly, evidence of current practice, as well as precedent, are used by the courts to determine what the terms of the relationship between bank and customer are. The Code is now the primary evidence of this current banking practice. It may also be evidence of customers' reasonable expectations which, if relied upon to the detriment of the customer, may result in the bank being estopped from contravening its provisions.[43]

Lastly, but very significantly, is the voluntary creation by the banking industry of the Banking Ombudsman scheme, which came into effect on 1 July 1992. The Banking Ombudsman's task is to resolve, in a non-adversarial manner, disputes which remain deadlocked after the bank's own internal complaints procedure has been exhausted. Bank customers do not have to pay for this service, as the scheme is fully funded by the participating banks. The complete independence of the Banking Ombudsman is, moreover, assured by the placing of the Banking Ombudsman Commission between the Ombudsman and the participating banks. The Commission comprises a neutral Chairman, two members from the banks, one person nominated by the Minister of Consumer Affairs, and the Executive Director of the Consumers' Institute or other customer representative.

The first Banking Ombudsman, appointed for an initial period of two years, is Mrs Nadja Tollemache. Her reputation, built up over the past five years as an Ombudsman reporting to Parliament, is likely to inspire confidence in and respect for the scheme on the part of banks and customers alike.

The Banking Ombudsman is likely to hold the banks strictly to the letter of the Code in resolving disputes, since she will treat the provisions as implied terms of the contract. The formal sanctions available to the Ombudsman are few; the role is mainly a recommendatory one. However, if a

---

43 Miller, as note 42, page 3.

recommendation is accepted by the complainant but not by the bank within one month of being made, the Ombudsman may make a binding award against the bank.[44] The award shall not exceed $100,000 and shall only be sufficient to compensate the customer for direct loss or damage suffered by reason of the acts or omissions of the bank.[45] Awards will probably be rare; the British Banking Ombudsman (a similar non-statutory scheme) reported that so far no bank has refused to accept any formal recommendation made by the Banking Ombudsman.[46]

All this has considerable importance for customer data privacy. The Code does more than set out formerly accepted standards of banking practice. It also significantly alters the status quo in some respects, particularly, from the point of view of this paper, the inclusion of provisions for the protection of customer information.[47]

A summary of the Code's provisions shows that the banks have modelled their approach fairly closely on the privacy principles as given in the Privacy of Information Bill:[48]

> Personal information is to be collected for the purposes of establishing and maintaining relationships with customers.
>
> Customer consent is required before information is used for purposes other than that for which it was collected "or related purposes".
>
> Banks are to take all reasonable steps to ensure that information is accurate, complete and up-to-date.
>
> Disclosure is only allowed in situations covered by the Tournier qualifications.

---

44 The banks are deemed to have undertaken to be bound by an award under the Rules of the Banking Ombudsman Commission, para. 16.3.

45 Terms of Reference for the Banking Ombudsman, para 14

46 Seventh Report of the UK Banking Ombudsman.

47 Code of Banking Practice, para. 10.

48 See Appendix A.

Third parties to whom disclosures are made may be asked to treat the information as confidential.

Customers are to have access to their personal information. This will include address, occupation, marital status, age, sex, accounts held, their balances and statements. Access is to be given within a reasonable time. Banks may recover the costs of supplying the information.

The customer has the right to reasons for denial of access to personal information and to challenge the denial through internal complaints procedures.

He or she also has the right to require correction of records, which must be amended accordingly. If incorrect information has been released to third parties, banks are to take all reasonable steps to inform those parties of the necessary corrections.

A close examination of the provisions reveals that the scope of some of them is rather unclear and that improvements could be made. First, it should be made clear that information will only be used for the purposes for which it was collected or for directly related purposes. The wording of the Code at present may allow use for indirectly related purposes. Another ambiguity is the use of 'consent' without stating whether express, or merely implied consent is required.The reference to the Tournier consent qualification certainly includes implied consent. However, implied consent may be inappropriate when dealing with use of customer information or the giving of bankers' references, and causes problems with disclosure itself.[49] Much of the documentation used by the banks contains references to collecting information from, or releasing it to, third parties. It is suggested that in order for express consent to be given by

---

49 See above, Part II.

the customer, it may be necessary for the bank to point out the fine print specifically and receive authorisation.

Secondly, the Code provides that the customer has a right of access to his or her personal information. However, the list of information available, while not exhaustive, would seem only to give the customer the chance to check that these non-controversial data are correct. Information such as assessments of creditworthiness contained, for example, in diary notes may not be accessible, although inaccuracy in this respect would be far more damaging to the customer than ~~that~~ in those categories listed. It is clearly envisaged that there may be circumstances in which the bank will wish to deny access, but possible good reasons for denial are not specified. This neither aids the customer, nor gives a basis for a decision under the internal complaints procedure or before the Banking Ombudsman.

These shortcomings, however, by no means destroy the basic merit of the provisions, which give the customer significantly improved privacy protection. The banks have voluntarily taken an important first step towards comprehensive data protection. In some cases, the obligations undertaken to the customer are fairly onerous.[50]

The action of the banks is to be applauded.

---

50 For example, the obligation to take all reasonable steps to keep records accurate, complete and up-to-date. The onus is thus shifted from the customer, who previously had to notify the banks of changes, to the bank itself. What 'reasonable steps' will entail is of course an open question.

III THE NEED FOR DATA PRIVACY LEGISLATION

The opening statement of paragraph 10 of the Code of Banking Practice declares firmly:

> The following provisions relating to the protection of customer information have been drafted prior to the coming into effect of any privacy of information legislation and will be reviewed on the enactment of any such legislation to ensure that they conform with the provisions of that legislation.

This seems to recognise the probability of an eventual enactment of the Privacy of Information Bill, while also demonstrating the goodwill of the industry. Inherent in it too, perhaps, is a certain amount of confidence that little would need to be changed in the event of the Bill becoming law, since the Code's provisions are clearly modelled on the privacy principles at the heart of the Bill. It is suggested, however, that there are significant differences between the Code and the Bill. In some respects, the Bill would provide greater protection than the Code. However, it cannot be ignored that there are flaws in the drafting of the Bill which seriously undermine the protection afforded. Nevertheless, the writer firmly believes that legislative intervention is not only desirable but vital in today's data controlled society.

The disadvantages of the Code when compared with the Bill

First, there is no provision in the Code of Banking Practice that personal information must generally be collected directly from the individual concerned. Banks are therefore free to collect information about their customers from any outside source. This is frequently useful in supplementing information already held by the bank. Credit reference agencies, for example, are among the principal outside sources of information to which banks gain access. Principle 2 of the Bill, however, would limit a bank's ability to collect personal information from third parties mainly to

situations where :

a) the information is already publicly available;
b) the customer authorises the collection;
c) collecting data directly from the customer would prejudice the purposes of the collection.[51]

It is submitted that it would not be unreasonable to require that customers authorise the collection of data from outside sources. Any data which the bank considers to be very highly sensitive are likely to fall within exception c). Perhaps in the majority of cases, consent will effectively have to be given in order to obtain a desired service. For example, a bank may wish to obtain information from a credit reference agency before granting a loan facility. If the customer authorises this,[52] then she or he is at least aware thereafter of the existence of that information in the bank file. If a decision is taken which is unfavourable to the customer, she or he may then request access to the information to check its accuracy and if necessary require correction of errors.

Secondly, there are no real provisions in the Code for the safe storage of customer data. Paragraph 10.1 states that "strict internal rules on the use, availability and access to information held on customers" will be imposed by banks. This falls short of Principle 5 in the Bill, which requires that "information is protected by such security safeguards as it is reasonable in the circumstances to take against:

(i) Loss; and
(ii) unauthorised access, use, modification or disclosure; and

---

51 The writer's criticism of the exclusion of publicly available information from the protection of the Bill is noted below.

52 See above, Part II. For this to be effective, the bank should specifically point out the relevant clause of the documentation and gain express consent.

(iii) other misuse.

In practice, most banks are extremely security-conscious, and such a duty might seem to be superfluous. However, mistakes occur, such as angling VDU screens on tellers' desks in such a way that other customers can see the information on them. Adhering to the requirements of safe storage should not be too onerous for the banks. Also, if it can be shown that divulgence of or interference with personal data was caused by lax security standards, a remedy should be available to the customer which the Code may not provide.

Thirdly, the Code, as mentioned above, is not specific as to what reasons might allow a bank to deny a customer's request for access to personal information. Acceptable reasons for denying access under the Bill are stated in Parts IV and V. These have been taken from the Official Information Act, where they have not proved to be unduly restrictive for the person requesting information. The reasons in the Bill for denial of access include, in clause 27 (1)(b) situations where making the information available "would be likely unreasonably to prejudice the commercial position of the person who supplied ... the information". This may be overridden by considerations of public interest, however. Banks and customers would therefore both be adequately protected under the legislation. As it stands, however, the scope of what the banks might term "good reasons" for denying access under the Code may be just as wide or as narrow as the banks themselves wish. It is difficult to see the provisions of the Code as giving sufficient certainty of access for the 'right' to have much meaning. The legislation would give that certainty.

Lastly, there is a wider range of remedies available to a natural person whose privacy is breached under the Bill. The Human Rights Tribunal will have power to make legally binding decisions about complaints, and may make declarations or orders as specified in clause 73:

a) A declaration that the action of the defendant is an interference with the privacy of an individual;
b) An order restraining the defendant from continuing or repeating the interference, or from engaging in, or causing or permitting others to engage in, conduct of the same kind as that constituting the interference ...
c) Damages in accordance with clause 76 of the Act;
d) An order that the defendant perform any acts specified in the order with a view to remedying the interference or redressing any loss or damage suffered by the aggrieved individual as a result of the interference, or both.

The Tribunal may make an award of damages in accordance with clause 76 in respect of one or more of:

a) Pecuniary loss suffered as a result of, and expenses reasonably incurred by the individual for the purpose ofthe transaction or activity out of which the interference arose;
b) Loss of any benefit, whether or not of a monetary kind, which the aggrieved individual might reasonably be expected to obtain but for the interference;
c) Humiliation, loss of dignity, and injury to the feelings of the aggrieved individual.

The Banking Ombudsman, in contrast, may make a binding award only in respect of direct pecuniary loss. If such loss cannot be shown, and the bank refuses to accept a recommendation on recompense, the customer is left without a remedy. It is worth noting that the limit of damages in the legislation is much lower than that available from the Banking Ombudsman,[53] but the latter can adjudicate disputes

---

53 The limit of an award by the Ombudsman is $100,000; the Tribunal may award only up to $50,000 under cl. 76(2).

between companies as well as natural persons. The maximum in the Bill, however, relates to the most any one individual (natural person) can receive. Also, privacy issues are likely to form only a very small percentage of the complaints to the Banking Ombudsman and are less likely to involve very large sums of money than many other heads of claim. The introduction of the legislation would therefore greatly enhance the remedies open to an individual customer, who may not be able to show direct pecuniary loss, but who may have missed out on a job, a loan or a house sale, or have suffered severe humiliation as a result of a breach of privacy.

The shortcomings of the Bill

Despite the above remarks, however, it is recognised that the Bill is in some respects significantly flawed. If various deficiencies are not corrected before the Bill is enacted, it may well be that a bank customer whose privacy is breached by their bank would fare better in complaining to the Banking Ombudsman under the Code than to the Privacy Commissioner.

The first concern is that showing that a breach of the privacy principles has occurred does not in itself ensure that the aggrieved person will be entitled to a remedy. The complainant must also show, under clause 59, that, for example, the action interfering with privacy is contrary to law, or unreasonable, unjust or oppressive. While an individual may bring an action to the Tribunal himself or herself if the Privacy Commissioner declines to do so,[54] that person may have to bear the cost of proceedings under clause 73(2).[55] A breach of the provisions of the Code,

54 Privacy of Information Bill 1991, cl.71.

55 Report of the Chief Ombudsman and the Ombudsman to the Justice and Law Reform Committee on the Privacy of Information Bill, December 1991, 15.

however, will be viewed as a breach of the terms of the contract between bank and customer by the Banking Ombudsman. The complainant has less to prove, and the claim can be dealt with directly. The customer also does not have to shoulder any of the costs of the proceedings.

The second major concern, which affects the operation of the whole Bill, is its exclusion of "publicly available information" from the protection of the principles.[56] This was heavily criticised in the Ombudsmen's Report.[57]

> Examples of publicly available information include name, place and date of birth, parentage, marital status, children, address, occupation ... as well as particulars relating to the ownership of land, motor vehicles, secured debts, criminal records, bankruptcies, any history of tax evasion, directorships and company shareholding. Such information, if incorrect, incomplete or out of date can be extremely damaging. It should be accessible and subject to correction.

Indeed, none of the principles designed to protect the individual's privacy will apply to such information. The Ombudsmen noted the particular significance of this in respect of "credit reference agencies, financial institutions and the like."[58] Profile building from publicly available information constitutes a very grave danger to privacy.

Thirdly, under clause 31, a bank would be able "neither to confirm nor deny" the existence of information, if it is satisfied that, for example, its commercial position would be prejudiced by confirmation or denial. Unlike section 10 of the Official Information Act, however, which contains the

---

56 Privacy of Information Bill 1991, clause 4.

57 As note 55, page 6.

58 As above, note 55, page 13.

same provision, the clause in the Bill is non-reviewable. It would therefore be within the judgement of the bank alone whether its commercial interests justify non-confirmation. This may almost eliminate the 'right of access'.[59] Under the Code, however, the Banking Ombudsman may take into account any considerations which she feels are relevant. A 'neither confirm nor deny' statement, if that is possible at all under the Code, would be reviewable by her.

Finally, there are two relatively minor aspects in which the provisions of the Code are preferable to those in the Bill. The Bill does not apply to legal persons, but only to natural persons in the definition of 'individual' in clause 2. This is probably entirely appropriate for legislation with such wide coverage, for different considerations may need to be taken into account when dealing with data privacy of companies. However, the application of the Code and the Banking Ombudsman scheme to individuals and legal persons alike is a point in their favour.

Also, a major disadvantage to the banks under the proposed legislation is that, under clause 35, they would not be allowed to charge for making information available to customers. However, the Code in paragraph 10.5.2 allows banks to recover the costs of supplying information. The Banking Ombudsman can ensure that such charges are not excessive. The writer suggests that it would be unreasonable to expect banks to carry all the costs of access. The banks already have to cover the cost of the many thousands of inquiries from government departments under statute. Any increase in the banks' liability for such charges would inevitably lead to increased banking charges for the consumer.[60]

---

59 As above, note 55, page 14.

60 The Banking Ombudsman may then be unable to review the charges, as these could class as a general bank policy which does not in itself breach a duty owed to the complainant. Terms of Reference for the Banking Ombudsman, paragraph 20.

The need for legislation

It is suggested that it would be unfortunate if the Privacy of Information Bill were enacted in its present form, given its many failings. However, the writer contends that there is a great need for effective data privacy legislation in New Zealand. Priority should be given to making the necessary amendments to the Bill.

Self-regulation should be encouraged under any data privacy legislation, as it is both more cost-effective and more likely to achieve compliance from industry members (because of considerations of competition) than a government-imposed regime.[61] The Code of Banking Practice, with the few reservations noted above, is a good example of effective self-regulation in the information privacy field. However, this does not do away with the need for legislation. The Code itself, and participation in the Banking Ombudsman Scheme is still essentially voluntary. It is possible for a bank to withdraw and to go its own way, as one Australian bank has recently done. The customer is then left without a remedy for breaches of privacy, unless they are covered by the common law duty of confidentiality.

Also, many other data users do not subscribe to voluntary codes of practice. They do not at present have to conform to any standards of data privacy. For instance, if a bank is allowed to disclose information to a non-banking subsidiary, the information is then not covered by the Code and customer protection is lost. It must also be said that there are many irresponsible data users in the marketplace, and it is precisely they who are least likely to conform to voluntary self-regulation. Tighter, universal controls are essential if the present large number of privacy breaches in this country is to be reduced.[62]

---

61 A useful tool in encouraging self-regulation may be the provisions for exemptions from the strict letter of the legislation, set out in the Privacy of Information Bill, Part VI. Space does not allow full consideration of this issue here, however.

62 Consumers' Institute Consumer, January 1991, 3.

New Zealand must also be aware of the international pressure to enact data privacy legislation. As a signatory to the OECD Guidelines, although not legally bound, we should not be seen to be refusing to act. The risk of being "frozen out" of the international info-technology market, with the consequent economic impact, cannot be ignored.

IV CONCLUSIONS

The banking industry has shown itself to be aware of the growing concerns, both public and political, about potential invasion of data privacy. The provisions in the Code of Banking Practice are a useful step in the right direction towards protecting customers' personal information. The requirements of the Code go far beyond any previous obligations of banks to their customers, and this is to be applauded.

While it is not strictly a legally binding document, the banks would be well advised to treat the provisions of the Code as if they had legal effect. The Banking Ombudsman is likely to treat the Code's provisions as implied terms of the contract between bank and customer, and will make her recommendations and awards on that basis. The Code will also constitute the primary evidence of current banking practice which the courts employ, together with precedent, in deciding whether a bank is in breach of its contract with the customer.

While self-regulatory measures such as those adopted by the Bankers' Association are entirely to be encouraged, data privacy legislation is still necessary. As it stands, however, the Privacy of Information Bill is inadequate to meet the needs of data subjects in this country. Indeed, the Code, especially as administered by the Banking Ombudsman, is in some respects ~~is~~ better able to protect bank customers from breaches of privacy by their banks.

Necessary amendments to the Bill should be made, such as making breaches of the privacy principles more directly actionable, including publicly available information within the scope of the legislation, and making clause 31 reviewable by the Privacy Commissioner. If this is done, we shall be well on the way to having effective data privacy protection which accords with our international undertakings, and adequately protects data subjects without harming the interests of commerce.

an unincorporated body (being a board, council, committee, subcommittee or other body)—

(i) Which is established for the purpose of assisting or advising, or performing functions connected with, any agency; and

(ii) Which is so established in accordance with the provisions of any enactment or by any agency,—

shall be treated as having been done by, or disclosed to, the agency.

Cf. Privacy Act 1988 (Aust.), s. 8 (1)

7. Act to bind the Crown—This Act binds the Crown.

PART II

Information Privacy Principles

8. Information privacy principles—The information privacy principles are as follows:

INFORMATION PRIVACY PRINCIPLES

Principle 1

Purpose of collection of personal information

Personal information shall not be collected by an agency unless—

(a) The information is collected for a purpose that is a lawful purpose directly related to a function or activity of the agency; and

(b) The collection of the information is necessary for, or directly related to, that purpose.

Principle 2

Manner of collection of personal information

(1) Where personal information is collected by an agency, that information shall be collected—

(a) Directly from the individual concerned; and

(b) With the knowledge or consent of the individual concerned.

(2) The collection of information other than in compliance with **subclause (1)** of this principle is not a breach of that principle if—

(a) The information is already publicly available; or

(b) That non-compliance is authorised by the individual concerned; or

(c) Compliance with **subclause (1)** of this principle would prejudice the purpose of the collection; or

(d) That non-compliance would not prejudice the interests of the individual concerned; or

(e) That non-compliance is required or authorised by or under law; or

(f) Compliance with the requirements of **subclause (1)** of this principle is not possible in the circumstances of the particular case.

(3) Personal information shall not be collected by an agency—

(a) By unlawful means; or

(b) By means that, in the circumstances of the case, are unfair.

PRINCIPLE 3

Solicitation of personal information from individual concerned

(1) This principle applies where—

(a) An agency collects personal information; and

(b) The information is solicited by the agency from the individual concerned.

(2) Where this principle applies, the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected or, if that is not practicable, as soon as practicable after the information is collected, the individual concerned is aware of—

(a) The purpose for which the information is being collected; and

(b) The intended recipients of the information; and

(c) The name and address of—

(i) The agency that is collecting the information; and

(ii) The agency that will hold that information; and

(d) If the collection of the information is authorised or required by or under law,—

(i) The fact that the collection of the information is so authorised or required; and

(ii) Whether or not disclosure by that individual is voluntary or mandatory; and

(e) The consequences (if any) for that individual if all or any part of the requested information is not provided; and

(f) The rights of access to and correction of personal information provided by these principles.

(3) It shall not be necessary for an agency to comply with a requirement of **subclause (2)** of this principle if to do so would frustrate the purpose of the collection.

PRINCIPLE 4

Solicitation of personal information generally

Where—

(a) An agency collects personal information; and

(b) The information is solicited by the agency,—

the agency shall take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected,—

(c) The information collected is relevant to that purpose and is up to date and complete; and

(d) The collection of the information does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

PRINCIPLE 5

Storage and security of personal information

An agency that holds personal information shall ensure—

(a) That the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against—

(i) Loss; and

(ii) Unauthorised access, use, modification, or disclosure; and

(iii) Other misuse; and

(b) That if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.

PRINCIPLE 6

Information relating to personal information kept by agency

(1) An agency shall maintain a document setting out—

(a) The nature of the personal information held by the agency; and

(b) The purpose for which each type of personal information is held; and

(c) The classes of individuals about whom personal information is held; and

(d) The period for which each type of personal information is kept; and

(e) The persons who are entitled to have access to that personal information and the conditions under which they are entitled to have that access; and

(f) The steps that should be taken by individuals wishing to obtain access to that information; and

(g) A description of the information matching programmes in which that agency is involved.

(2) An agency shall—

(a) Make the document maintained under **subclause (1)** of this principle available, on request, for inspection by members of the public; and

(b) If requested by the Commissioner, give the Commissioner a copy of the document so maintained.

(3) Where there is good reason under **section 26 or section 27** of this Act for withholding information, nothing in **subclause (1)** of this principle requires the inclusion of that information in the document maintained under that subclause.

(4) Nothing in **subclause (1)** of this principle requires an agency to include in the document maintained by it under that subclause, in respect of any information matching programme, any information the disclosure of which would be likely to frustrate the object of the programme.

PRINCIPLE 7

Access to personal information

(1) Where an agency holds personal information in such a way that it can readily be retrieved, the individual concerned shall be entitled—

(a) To obtain from the agency confirmation of whether or not the agency holds such personal information; and

(b) To have access to that information.

(2) Where, in accordance with **subclause (1) (b)** of this principle, an individual is given access to personal information, the individual shall be advised of that individual's rights, under **principle 9**, to request the correction of that information.

(3) The application of this principle is subject to the provisions of **Parts IV and V** of this Act.

PRINCIPLE 8

Access to reasons for decisions

(1) Where an agency (being a Department or a Minister or an organisation or a local authority) makes or has made, in respect of any individual, a decision or recommendation, being a decision or recommendation in respect of that individual in his or her personal capacity, that individual is entitled to and shall,

on request made within a reasonable time of the making of the decision or recommendation, be given a written statement of—

(a) The findings on material issues of fact; and

(b) Subject to **section 28 (1) (b) to (e)** of this Act, a reference to the information on which the findings were based; and

(c) The reasons for the decision or recommendation.

(2) Nothing in this principle entitles any individual to obtain a written statement of advice given to the Sovereign or the Sovereign's representative.

(3) Nothing in this principle applies in respect of any decision or recommendation made by the Public Trustee or the Maori Trustee—

(a) In his or her capacity as a trustee within the meaning of the Trustee Act 1956; or

(b) In any other fiduciary capacity.

(4) The application of this principle is subject to the provisions of **Parts IV and V** of this Act.

PRINCIPLE 9

Correction of personal information

(1) Where an agency holds personal information, the individual concerned shall be entitled—

(a) To request correction of the information; and

(b) To request that there be attached to the information a statement of the correction sought but not made.

(2) An agency that holds personal information shall, if so requested by the individual concerned or on its own initiative, take such steps (if any) to correct that information as are, in the circumstances, reasonable to ensure that—

(a) The information is accurate; and

(b) Having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, the information is relevant, up to date, complete, and not misleading.

(3) Where an agency that holds personal information is not willing to correct that information in accordance with a request by the individual concerned, the agency shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the information any statement provided by that individual of the correction sought.

(4) Where the agency has taken steps under **subclause (2) or subclause (3)** of this principle, the agency shall, if reasonably

practicable, inform each person or body or agency to whom the personal information has been disclosed of those steps.

(5) Where an agency receives a request made pursuant to **subclause (1)** of this principle, the agency shall inform the individual concerned of the action taken as a result of the request.

PRINCIPLE 10

Agency to check accuracy, etc., of personal information before use

An agency that holds personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up to date, complete, and not misleading.

PRINCIPLE 11

Agency not to keep personal information for longer than necessary

An agency that holds personal information shall not keep that information for longer than is required for the purpose for which the information was obtained or for any other purpose for which the information may lawfully be used.

PRINCIPLE 12

Personal information to be used only for relevant purposes

An agency that holds personal information shall not use the information except for a purpose to which the information is relevant.

PRINCIPLE 13

Limits on use of personal information

An agency that holds personal information that was obtained for a particular purpose shall not use the information for any other purpose unless—

(a) The use of the information for that other purpose is authorised by the individual concerned; or

(b) The agency believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another individual; or

(c) The purpose for which the information is used is directly related to the purpose for which the information was obtained; or

(d) Use of the information for that other purpose is required or authorised by or under law; or

(e) Use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

(f) The information—

(i) Is used in a form in which the individual concerned is not identified; or

(ii) Is used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or

(g) The use of the information is for the purposes of an information matching programme approved by the Commissioner pursuant to **section 92 (1) (a)** of this Act.

PRINCIPLE 14

Limits on disclosure of personal information

(1) An agency that holds personal information shall not disclose the information to a person or body or agency unless—

(a) The disclosure is to the individual concerned; or

(b) The disclosure is required or authorised by or under law; or

(c) The purpose for which the information is disclosed is directly related to the purpose for which the information was obtained; or

(d) The disclosure is made pursuant to any provision of the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987; or

(e) The disclosure is authorised by the individual concerned; or

(f) The agency believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another individual; or

(g) The disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty; or

(h) The information—

(i) Is to be used in a form in which the individual concerned is not identified; or

(ii) Is to be used for statistical or research purposes and will not be published in a form that could

reasonably be expected to identify the individual concerned; or

(i) The disclosure is made for the purposes of an information matching programme approved by the Commissioner pursuant to **section 92 (1) (a)** of this Act.

(2) Nothing in **subclause (1)** of this principle shall be taken as authorising the disclosure of any personal information in any case where the disclosure of that personal information would be a breach of any obligation of secrecy or non-disclosure imposed by the provisions of any enactment.

9. Application of information privacy principles—(1) **Principles 1, 2, 3, 4, and 13** apply only in relation to information collected or obtained after the commencement of this Part of this Act.

(2) **Principles 5 to 7, 9 to 12, and 14** apply in relation to information held by an agency, whether the information was collected or obtained before, or is collected or obtained after, the commencement of this Part of this Act.

(3) **Principle 8** applies only in relation to—

(a) Decisions or recommendations made on or after the 1st day of July 1983 by a Minister or a Department or an organisation; and

(b) Decisions or recommendations made on or after the 1st day of March 1988 by a local authority.

Cf. Privacy Act 1988 (Aust), s. 15

10. Enforceability of principles—(1) The entitlements conferred on an individual by **subclause (1)** of **principle 7** (in so far as that subclause relates to personal information held by an agency that is a Minister, a Department, an organisation, or a local authority), and by **principle 8**, are legal rights and are enforceable accordingly in a Court of law.

(2) Subject to **subsection (1)** of this section, the information privacy principles do not confer on any person any legal right that is enforceable in a Court of law.

PART III

PRIVACY COMMISSIONER

11. Privacy Commissioner—(1) There shall be a Commissioner to be called the Privacy Commissioner.

(2) The Commissioner shall be appointed by the Governor-General on the recommendation of the responsible Minister.

(3) The Commissioner shall be a corporation sole with perpetual succession and a seal of office, and shall have and

APPENDIX B
CODE OF BANKING PRACTICE

10.0 PROTECTION OF CUSTOMER INFORMATION

The following provisions relating to the protection of customer information have been drafted prior to the coming into effect of any privacy of information legislation and will be reviewed on the enactment of any such legislation to ensure that they conform with the provisions of that legislation.

10.1 Banks will impose strict internal rules on the use, availability and access to information held on customers and former customers and adhere to all legislation relating to information privacy.

10.2 Banks will require all of their employees to sign a declaration of secrecy.

10.3 Use of Customer Information

10.3.1 Banks will collect personal information for the purpose of establishing and maintaining relationships with customers, including the protection of customers' and banks' interests. Before personal information is used for purposes other than those for which it was collected, or related purposes, consent will be obtained from the bank's customers.

10.3.2 Banks will take all reasonable steps to ensure that information on customers held in bank files is accurate, complete and up-to-date.

10.4 Areas where Disclosure of Customer Information May Occur

10.4.1 Banks will treat all personal information as confidential. However, there are four circumstances in common law under which such information may be disclosed to third parties. These are a follows:

(i) where the customer consents to the information disclosure;

(ii) when required to disclose the information by compulsion of law (a list of the Statutes that permit or require disclosure of confidential information is attached in the annex to this Code. The Statutes allow the individuals and organisations listed access to banks' confidential information). Where not prohibited by law, customers may be notified that a disclosure order has been received by the bank;

(iii) to protect banks' interests. For example, banks may pass information to Credit Reference Agencies about debts of customers who are in default or banks may disclose information to their solicitors and to debt collecting agencies when it is necessary to recover money owed to them; and

(iv) as an act of public duty. In exceptional circumstances, banks may be under a public duty to disclose personal

information to appropriate authorities in matters of significant public interest. For instance, where a bank has reasonable and probable grounds for believing there is an attempt to use its facilities for criminal activity such as the laundering of the proceeds of organised crime.

10.4.2 Banks will not provide bankers' references without the prior consent of the customer on whom the reference is to be based.

10.4.3 Where disclosure to third parties is made, the bank will, where appropriate, request such parties to treat the information as confidential.

10.5 **Customer Access to Their Personal Information**

10.5.1 Banks will provide, upon customer request:

(i) Confirmation as to whether specific personal information about that customer is held by the bank; and

(ii) access to personal information held about that customer which will include address, occupation, marital status, age, sex, accounts held, their balances and statements.

10.5.2 The information will be provided within a reasonable time. Baks may recover the costs of supplying this information. If a request is denied, the customer has the right to be given reasons for the denial, and the right to challenge the denial through the bank's internal complaints procedures (see Part III of the Code).

10.5.3 Customers have a right to request (or require) correction of personal information about them in bank records. Banks will amend incorrect or incomplete information about customers. Where incorrect or incomplete personal records have been disclosed to third parties, banks will take all reasonable steps to inform those third parties of the necessary corrections.

10.6 **Direct Marketing of Services**

10.6.1 Banks will act responsibly in the use of direct marketing, and will also recognise the Codes of Ethics of the New Zealand Direct Marketing Association.

1 Folder Sh

Sharp, Katrine Elisabeth
Cheques and balances