Privacy Policies And Practices: An Investigation of Secondary Use of Information within South African Retail Banking Institutions

JITHENDRA CHOTOO DAYA

A research report submitted to
the Faculty of Commerce,
University of the Witwatersrand,
Johannesburg, in the partial fulfilment
of the requirements for the degree
of Master of Commerce

Declaration

I declare that this research report is my own unaided work. It is being submitted for the degree of Master of Commerce in the University of the Witwatersrand, Johannesburg. It has not been submitted for any degree or examination in any other University.

JITHENDRA CHOTOO DAYA

DATE : 29 November 1996

Abstract

This paper addresses concerns surrounding information privacy and the secondary use of information in South African corporations. This study also attempts to assess the level of concern that management and information technology practitioners in South African retail banks have about privacy issues.

The research suggests that privacy is a huge concern internationally and may affect South African corporations if they do not follow certain policies and practices. Eleven in-person structured interviews were conducted at four banks.

The research proposes a set of guidelines by which South African management and IT practitioners, who are involved with the identification and solution of some of the problems that may be presented by possible privacy legislation, will be able to assess their policies and practices against international practices and policies. The results inform IS managers and executives about appropriate business policies they can implement voluntarily to address public concerns about specific information practices that may be considered a threat to privacy.

The findings suggest that the executives are deliberately avoiding confronting the issue of information privacy for as long as possible. The executives are adopting a wait-and-see attitude and will react on whatever legislation requires them to do. At the time of the report senior executives at banks were not accepting responsibility for information privacy policies and practices and were leaving this responsibility to the middle level managers who implement their own practices based on their own needs.

Acknowledgements

I thank my family for being so patient with me during the research and writing of this thesis. I also thank Ms Frances Sutherland and Professor Arthur Money for their guidance during the initial phases of this project. I am most indebted to my supervisor for this study, Mr Tom Addison, for his guidance and comments, and to the interviewees and their companies for their participation and co-operation.

Table of Contents

List of tables

1.0. Introduction

The advent of the Information Age raises a number of new issues. One of the most important of these is how to deal with information as a valuable resource. As organisations become more information-intensive, managers find themselves in a fascinating but baffling world of sophisticated information technologies (IT). These new technological capabilities are making new applications possible. Also, the capacity of computers to store information on an unlimited range of subject matters has increased dramatically. Information held contains both commercial and personal information, some of which is private information and some is available publicly.

Information considered personal and private is being collected, collated, and sold. These activities occur with or without the consent of individuals. The lucrative opportunities in the information services business have attracted the interest of many companies that have their primary business in other areas. Supermarkets, financial institutions, magazines, mail order houses, and even doctors have learned that the data they routinely accumulate about their customers has considerable value to other organisations. Personal information such as income, marital status, credit history, medical records, political party, employment history, military history, and school history is collected and stored in various databases. Much of this personal information is used for purposes that were not originally intended (Straub and Collins, 1990; Smith, 1993; Page, 1994).

Secondary information use occurs when personal information collected for one purpose is subsequently used for a different purpose. While secondary information use is both widespread and legal, it may be viewed as an invasion of *privacy* when it occurs without the knowledge or consent of the individual whose details are being used.

Detailed knowledge about individual preference is increasingly valuable to decision makers in the competitive global economy. Advances in IT facilitate the collection and use of this information. However, it may be difficult for firms to pursue the opportunities enabled by technology without risking a public, client or consumer backlash if the applications do not reflect a common set of values or a shared understanding about *privacy*.

1.1. Background

Privacy is a complex concept and has been defined in various ways. Information privacy, defined as a condition of limited access to identifiable information about individuals (Smith, 1993), is concerned with the proper handling and protection of personal information, such as information about employees, customers, clients or consumers.

The concept of privacy as a separate right was first articulated over 100 years ago. Since then advances in electronics, computers and other technologies have accentuated privacy concerns in two broad arenas - surveillance and personal data protection.

Currently, there is no legislation or self-regulating policies with regard to data/information privacy in South Africa. The legislatures in many other countries recognise both the political and emotional value of privacy protection and have adopted a variety of strategies for achieving meaningful protection (Rotenberg, 1995). At the heart of these efforts are a set of guiding principles concerning collection, use and dissemination of personal information.

Overseas' governments, industry, and academic sources suggest that (consumer) privacy has become a critical public policy topic (Goodwin, 1991). Due to its intimate connection with the personal finances of most customers, the banking industry faces higher consumer expectations regarding privacy than any other industry because consumers are increasingly concerned about who has access to their financial information and how it's being used (Kearney, 1995). Privacy protection requires disclosure to consumers of the way information will be disseminated and used as well as about limits on collection and storage of data. The legislative trend in the majority of the countries in

Europe, the United States of America and in the United Kingdom reflects movement toward acceptance of privacy as a consumer right (Katz and Tassone, 1990).

The Association of Computing Machinery (ACM) is an international body that is concerned with all aspects of IT. It is concerned with the forces that will shape evolution of future technologies, the competence and integrity of individuals involved in IT, and the impact of these technologies on society. The ACM Code of Professional Conduct is in favour of the protection of individual privacy and it is supported by the International Federation of Information Processing (IFIP), to which the Computer Society of South Africa is affiliated.

1.2. The Relevance of this research

Gaining strategic advantage through information technology often depends upon effective secondary use of information by managers within the organisation (Porter and Miller, 1985; Burns and McFarlan, 1987; Culnan, 1989).

While privacy is clearly a strategic issue for organisations, it should be a priority for information systems management as well (Mason, 1986, Cappel, 1993). As a company's information steward with a broad view of the business, the chief information officer should be in the best position to help his or her firm avoid the crises faced by companies with regard to information privacy issues.

Mason (1986) asserts that because few legal restrictions apply to the gathering and use of personal information, privacy is an ethical issue as well as a business issue. He goes on to argue that information privacy is a growing concern and may prove to be the most important ethical issue of the information age.

These issues are important to South African IT professionals, direct marketers and holders of this type of information, as international privacy policies may be forced upon them, naving various implications. Concerns about violation of intellectual property rights and individual rights of privacy are important precisely because there are no clear-cut ethical frameworks in the computing professions to guide conduct in South Africa.

1.3. The problem

Information in South Africa can currently be given freely or collected without a person's consent. Personal information is usually given freely when people apply for credit, a mortgage, health insurance, hospital admittance, or decide to rent a video or register the warranty on a new purchase. Little of this information remains confidential (Page, 1994). Additional information is obtained through monitoring of cordless or cellular telephones or by the collection of information by credit bureaus, medical information bureaus and list brokers. Businesses buy or trade information about customers for direct mail or telephone solicitations

In recent years a new term has invaded the marketing literature, database marketing. To many direct marketing practitioners database marketing is another term for mailing list management. To others it is customer knowledge as part of a marketing information system, to be used fo business development and strategic planning (Fletcher et al., 1994).

It is becoming easier to collect personal information using new technologies e.g., point of sale systems. Improvements in speed and cost make cross-classifying information about individuals easier, thus enabling *computer-matching* processes (Kusscrow, 1984; Shattuck, 1984). Also, increased capabilities in telecommunication networks and standardised query languages for relational databases enable the merging of disparate bodies of information.

Such technological capabilities come at a time when the value of personal information is increasing in the marketplace. A shift from generalised to targeted marketing is an acknowledged trend (Cespedes and Smith, 1993), and additional personal information is required to effect the targeting efforts.

The variety of new information technologies that have emerged can improve the efficiency and effectiveness of marketing programs. However, the use of technologies such as computer matching, which compares data bases to identify individuals common to both, to support marketing problems also can lead to legal and societal difficulties (Bloom et al., 1994). The computer's unique capabilities for matching and statistical inference on large databases increases the threat to individual privacy. Such matching creates new information.

The change has brought with it new responsibilities of organisations to design adequate safeguards to protect against wrongful use of information. Much of the responsibility for this rests with information systems (IS) management. IS managers must become acutely aware of potential legal liabilities and how their organisations can best be protected from such risks (Straub and Collins, 1990). Straub and Collins (1990) suggest that IS managers have and will continue to have oversight responsibility for information liability.

Management is likely to exert more pressures for better control from IS management due to increasing public awareness, the potential for larger losses, and new legal responsibilities for assuring adequate information privacy protection (Canning, 1986). One of the main areas of concern for all managers is how to collect and disseminate information on individuals while respecting individual rights to privacy as there is a need to minimise the information liabilities of managers and their organisations.

The problem facing South African corporations is, because there is no legislation regarding information privacy, how will international privacy developments affect their opportunities to use new information technologies for marketing efforts. There are no available answers to the following potentially problematic issues which may pose huge problems in future:

- Will South Africa's national sovereignty be replaced by international sovereignty, i.e., international developments about providing and using personal information in databases will shape future legislation here - convergence of local laws toward international standards, hence this could limit the freedom to take advantage of technology for marketing purposes.
- Can data from abroad and/or South Africa be transferred back and forth if international principles are implemented here as well? What are the possible consequences if South Africa fails to do so?
- Can a corporation in South Africa sell their customer's information legally and ethically if South Africa does not follow the international privacy principles?
- How are South African corporations handling sensitive personal information today and are their practices and policies in line with the current international trends?
- How are South African corporations crafting the policies and practices that govern the use of sensitive personal information, and again, are their practices and policies in line with the current international trends?

The above questions, although relevant, are very broad and in order to assess whether information privacy is of concern to South African corporations, the last two questions are examined in this study.

1.4. Research objectives

As data privacy policies and practices are of great concern in the international arena, this research aimed at establishing whether data privacy is an issue or of concern to South African financial institutions or not. This was investigated in relation to managing the associated risks in compliance with both the observation of confidentiality of customer specific information and international privacy trends.

To address these issues, the following main questions were posed:

i) How are South African retail banks handling sensitive personal information today?

This question was used to help identify the level of concern that these corporations have regarding information privacy. It also established how well the current corporate policies and practices are meeting international societal expectations with respect to uses of personal information, for example credit information, medical information and information about one's purchases.

ii) How are South African retail banks crafting the policies and practices that govern the use of sensitive personal information?

Here the process through which information privacy policies and practices are created in these corporations was evaluated in comparison to international policies and practices.

2.0. Literature review

Computer technology affects every aspect of people's lives today (Page, 1994). The evolving information infrastructures within organisations, created by advances in technology, is expanding the level of interactivity, enhancing communication, and allowing for easier access to services and products (Agranoff, 1991). As a result, many more users are and will discover new, previously unimagined uses for customer information.

The recent advancements in database technology and information access have given rise to a growing misperception among consumers and regulators (direct marketers and the government) regarding the type and extent of customer's personal information and it's use (Fletcher et al., 1994). As companies make more use of information systems to run their business, sell services, offer advice, design products, and add value to their goods, there is a greater likelihood that poor information practices could lead to harm - to themselves or the customers (Dentino, 1994). Protecting personal data is one area in which legal issues are most likely to appear (McNurling, 1988).

Personal details are available to anyone willing to spend time, effort and money to find out this information. The availability of certain types of information may invite unsolicited telephone calls, hate mail or even death threats. Unauthorised usage of such information may have financial, political or personal consequences (Hughes, 1991).

> *"It isn't the technology that's the villain here, but the people who may misuse it"* (Seymour, 1991).

Today knowledge workers must look beyond the firm to satisfy their information needs. Developments such as executive information systems, computer-networks, electronic bulletin boards, and end-user computing demonstrate the scope of this change. Also indicative of this transformation is the need of top managers for information external to the organisation (Straub and Collins, 1990). In response to this technological change, overseas laws concerning information use have also undergone dramatic change.

The need for computer privacy is also seen as important with more people having direct access to information (Burrows, 1994).

2.1. Privacy in general

Privacy has been defined in various ways as: privacy is the right not to be disturbed or the right to be alone, the right not to be known or the right to be anonymous, the right not to be monitored or the right to intimacy, and the right not to have one's identifying information exploited or the right to control one's personal information (Gattiker, 1995(a)). In its broadest sense, it refers to the right of an individual or company to be protected against unwarranted intrusions into and unwarranted publicity about their lives

(Milne, Bloom and Adler, 1994). Privacy has also been described by some as the *kernel of freedom*, and the right from which other freedoms flow. According to Cespedes and Smith, 1993, privacy has two discrete components: physical privacy and information privacy. Physical privacy issues concern outcomes of database marketing processes (protection from unwanted telephone calls, mail and faxes). Information privacy issues concern the inputs, use and control of data. Information privacy is concerned with the proper handling and protection of personal information, such as information about employees, clients, customers or consumers.

Privacy has been associated with human dignity and respect for others (Goodwin, 1991). The concept of privacy as a separate right was first articulated over 100 years ago when then attorneys Brandeis and Warren wrote urging recognition of a right to privacy or as they phrased it, the *right to be let alone* (Tuerkheimer, 1993). Since then advances in electronics, computers and other technologies have accentuated privacy concerns in two broad arenas - surveillance and personal data protection.

Strategic uses of information technology based on personal information may raise privacy concerns among consumers *and holders of this information*, if these applications do not reflect a common set of values (Culnan, 1993; Neuman, 1994).

However, the privacy issues associated with the secondary use of information gathered as a result of these relationships have not been addressed explicitly. Instead, a number of studies have addressed the privacy issues associated with internal company policies for managing personal information (Woodman et al., 1982; Smith, 1993; Mazlin and Jamieson, 1994). Studies have also addressed privacy issues with regard to government information systems and governmental agencies using government/public data (Grupe, 1995).

Privacy is an important issue and the assault on privacy by technology has been predicted since the early 60s (Canning, 1985; Gattiker, 1995(b)). The primary force working against privacy is the fact that computer technology is getting better and cheaper, and more people have access to the technology.

> *"Software advances are making it easier for companies to piece together enough information to paint alarmingly detailed profiles of millions of individuals"* (Schwartz, 1992).

2.2. Privacy policies and practices

The legislatures in many countries recognise both the political and emotional value of privacy protection and have adopted a variety of strategies for achieving meaningful protection (Tuerkheimer, 1993). Although privacy as a legal right is traditionally associated with Western liberal countries, privacy is also described in the literature of many countries around the world. So widespread is the desire for privacy protection that several of the recently established democratic governments in Eastern Europe and former Soviet Union have included the right of privacy in their new constitutions (Rotenberg, 1993). More recently, the European nations have sought to develop a harmonised framework for data protection throughout the Eastern Community (Kearney, 1995). It is likely that this directive will have a substantial impact on the development of international privacy policy.

Current international trends in Europe in relation to privacy provide that if a country does not provide law to enforce an adequate level of data protection, then the country will no longer be allowed to receive transfers of personal information (Mazlin and Jamieson, 1994). This could have major effects on South African trade, communications, and professions such as IT professionals in both their professional work practices and in the amount of future work they will receive. To show this adequate level of protection a country must adopt compatible laws, or show an adequate level of protection through other means or exceptions (Neuman, 1994)

According to Culnan (1993), the Commonwealth Privacy Act 1988 requires that some changes are made to computer information systems in organisations and these changes are influenced by a number of privacy forces, internal and external, on an organisation (Mazlin and Jamieson, 1994). Some aspects of privacy legislation can be considered as enforcing good information handling practices. Even for the organisations that have these practices in place, privacy helps enforce these standards. The four areas of application that relate to information privacy principles which provide the basis for the Commonwealth Privacy Act are identified as : collection; storage ; usage ; and dissemination of personal information. Serious concerns regarding the collection and use of personal information deal with the following issues : how much incorrect information is kept in databases and how can the information be corrected?; what information is available and how is it obtained and used?; and, who has access to this personal information? (Page, 1994). Two major themes run through these principles. The first, is that information must be collected, used, and disseminated for a purpose that is legal and directly connected to the collector's function. The second, is that information upon collection, and before usage, should be checked for accuracy.

A 1990 *Draft Umbrella Directive on Data Protection* offered by the European Community has the following requirements: data use is prohibited without permission of consumers; data subjects must personally be notified to whom personal information has been passed and for what use; data subjects can claim compensation if data is *misused and caused damage*; and European Community data can be transferred out of the European Community only if the receiving country can guarantee the same level of protection (Bloom et. al., 1994).

Other nations like UK and Sweden have adopted broad data protection codes which may require data collectors to register with the government, or may impose a blanket prohibition on public and private data uses without the consent of the data subject (Vidmar and Flaherty, 1985).

[illegible] policies do exist, actual policies often [illegible] leaders in developing such policies; [illegible] being pressured by consumers, the [illegible] that as information technology [illegible] modify their approaches to [illegible] such as the creation of a [illegible] *principles*.

[illegible] with regard to [illegible] some of which [illegible] Commerce [illegible] Consumer Protection [illegible]

[illegible] aspect of the [illegible] The [illegible] that collect personal information [illegible] is also supported [illegible] is affiliated.

[illegible] disseminate [illegible] countries, [illegible] nies are [illegible] s and

[illegible] addressed [illegible] information [illegible] differentiating individuals [illegible] negative [illegible] concerned about [illegible] results [illegible] understanding [illegible] provided a basis [illegible] involving information.

[illegible] conducted a study amongst corporations [illegible] such as insurance companies [illegible] medical, financial, and consumer [illegible] comprehensive policies regarding [illegible]

There are various relevant legal statutes with regard to privacy threats and violating privacy rights in the United States of America, some of which are: Fair Credit Reporting Act (1970), Privacy Act (1974), Right to Financial Privacy Act (1978), Cable Communications Policy Act (1984), Computer Matching and Privacy Act (1988), Video Privacy Protection Act (1988), Telephone Consumer Protection Act (1991), State Caller ID Rules and State Privacy Laws.

Within the computing profession, one aspect of the ACM Code of Professional Conduct is the protection of individual privacy. The ACM Council took a position on privacy by urging members and organisations that collect personal information to observe the privacy guidelines (White, 1991). This stance is also supported by the IFIP to which the Computer Society of South Africa is affiliated.

2.3. Previous research models used

Culnan (1993), conducted a study that addressed what differentiates consumers who object to certain uses of personal information from those who do not object. Control emerged as a clear theme in differentiating individuals with positive overall attitudes toward secondary information use from those with negative attitudes. The study participants with positive attitudes were less concerned about privacy (measured as control over personal information), perceived shopping by mail as beneficial, and have coping strategies for dealing with unwanted mail. The results also suggested that theory related to categorisation of strategic issues as positive-negative with outcomes that were controllable/uncontrollable provided a basis for understanding differences in the ways individuals perceived practices involving information.

In another study, Smith (1994), conducted a study amongst corporations in America. He examined the policies of corporations such as insurance companies, banks, and credit card firms that regularly process medical, financial, and consumer data. The results indicate that many companies lack comprehensive policies regulating the access to and distribution of personal data, and where stated policies do exist, actual policies often conflict. Few organisations are willing to become leaders in developing such policies; instead they formulate privacy guidelines only after being pressured by consumers, the media, or legislators. Smith (1994), goes on to argue that as information technology advances, both corporations and society as a whole must modify their approaches to privacy protection. Specific policy suggestions were presented, such as the creation of a Data Protection Board, and a set of *generally accepted privacy principles*

2.4. Summary of Literature Review

Information technology makes it easier than ever to collect, store and disseminate personal information, then use it to carry out business decisions. In other countries, legislation limits corporate manipulation of personal data, and private companies are finding that they have to do the same or risk lawsuits from irate customers, clients and rejected prospects.

Various studies and papers have been written about information privacy. The general consensus is that information privacy is of great concern and that information technology use has a huge impact on information privacy. Society harbours expectations regarding corporate policies and the areas for concern are viz., improper information collection, new uses of information, sharing information, errors, improper internal access and reduced judgement. Professional bodies are urging members, organisations and IT professionals to observe stated privacy guidelines. Some overseas countries are forcing other countries to adopt an adequate level of data protection in order for that country to receive transfers of personal information.

With more people having direct access to information and the recent advancement in database technology, the need for information privacy is seen as important. The four areas of application that relate to information privacy principles which provide the basis for privacy legislation were identified as : collection; storage; usage and dissemination of personal information. This coupled with the lack of South African legislation covering the concerns raised regarding information privacy, initiated the questioning process that led to this study.

3.0. Research methodology

Banks regularly handle large amounts of personal information and use information technology extensively. They are also seen to be involved with database marketing and are constantly prospecting and targeting potential clients in addition to cross-selling products and services to existing clients. Because of the sensitive personal information of clients that banks hold in their databases and because they were viewed as being most likely to have confronted information privacy issues, banks have been chosen for this study. Banks A, B, C and E were targeted for this study as they are currently the four largest banks in South Africa. Due to the unwillingness of some of the potential interviewees from Bank E, Bank D was also targeted. These banks provide general retail, commercial and merchant banking services while also having credit card and insurance divisions.

One methodology considered for this study was the use of a mailed survey questionnaire to a sample of people. Surveys offer an opportunity to collect large quantities of data or evidence. Questionnaires also allow evidence to be gathered concerning *how much or how long or when* but are not really great value when the researcher is asking *how or why* (Remenyi, 1995). Remenyi (1995) asserted that as a general rule, the nature of the evidence which may be collected by means of a questionnaire is often regarded as relatively superficial especially in comparison to the evidence which is possible to collect from other techniques as personal interviews or case studies.

The methodology chosen for this empirical research was one of a qualitative nature rather than a quantitative nature. This was done by conducting semi-structured interviews with key people within retail banks in South Africa. This technique was also chosen due to the limited amount of time allocated to do the study in and the small number of institutions being targeted for this study. The strengths of this method is that it is targeted in that it focuses directly on the study topic and it is insightful as it also provides perceived causal inferences (Easterby-Smith et al., 1993). The weaknesses of this methodology, according to Easterby-Smith et al (1993), is that it could lead to bias due to poorly constructed questions, inaccuracies due to poor recall, and reflexivity in that the interviewee gives what the interviewer wants to hear. These limitations were considered during the structuring and testing of the interview schedule. Extensive written notes were taken during the interviews and observations were documented soon after the interviews.

3.1 Interview Schedule

Information regarding privacy policies and consumer concerns was gathered by extensive readings of literature available and previous research done outside of South Africa. An interview schedule was created and built on a previous research model used. The interview schedule was pre-tested on one-to-one interviews held with bankers in the field of direct marketing and information technology. The interview schedule was validated and questions that were to be posed during the interview were focused on privacy, direct marketing and the secondary use of information. The questions were directed to get an IT view, a marketing view and a general policy point of view. The following individuals were interviewed to test the interview schedule:

- two direct marketing managers from banks
- a direct marketing manager from the post office
- two students studying towards their Master in Commerce degree specialising in information technology ,
- one lecturer in the field of IT and marketing.

3.2 Interviewee selection

Interviewees received assurances that they would remain anonymous and that neither they or their banks would be quoted by name. Some of the people contacted within one bank, referred to as Bank E, refused to part-take in this study. The reasons being confidentiality, sensitivity and company policies. These responses were disturbing because: the study was totally anonymous, with the identity of all participants and their bank's details well protected; the requests were made at quite senior levels, and many of the senior executives from all other banks were in favour of the study. A summary of the participant refusals is shown in Table 1.

Table 1 - Participant Refusals

Level of contact	Reason for refusal
Divisional General Manager	Researcher works for an opposition bank
Senior Direct Marketing Manager	Against company policies
Information Technology Manager	Confidential/sensitive information

Within Bank B, a new division had been formed. This division is responsible for all the direct marketing efforts of the bank. This division employed new staff, not previously from Bank B, and new policies regarding customer information and privacy have been crafted. These policies are currently being formulated and the researcher has been involved with the formulation of these policies. Staff members within this division were not targeted for interviews as they were quite aware of this research and their input may be biased.

In most cases the request to conduct interviews with prospective participants was a cold contact, with the exception of Bank A and B with whom the researcher had previously worked.

The interviewees targeted for this research were therefore people working in the IT, marketing and general management fields of banking within South Africa. The interviews addressed the current policies and practices in the banks and the process of crafting information priva.y policies (interview summary in Table 2).

Table 2 - Interview Summary

BANK	Interviews Conducted	Number
Bank A	Direct Marketing	1
	Information Technology	1
	Retail Marketing	1
	Total	**3**
Bank B	Group Marketing & Sales	1
	Information Technology	1
	Group Projects	1
	Total	**3**
Bank C	Direct Marketing	1
	Information Technology	1
	Total	**2**
Bank D	Direct Marketing	1
	Executive Director	1
	Information Technology	1
	Total	**3**

The interviews in this study were semi-structured. Before each interview a protocol was constructed consisting of several questions that were to be posed to the interviewee. The specific list of questions depended on the individual's position and function within the organisation. Because of the sensitivity of the topic under research, the interviews were not tape-recorded. Detailed notes were written during the interview and additional observations were documented after the interview. Notes regarding the interview itself were made to indicate whether the interviewee appeared open and honest, and whether the interviewee's responses were in line with responses received from other interviewees from the same bank.

All questions from the interview schedule were posed. The varied sample of interviewees from the Marketing and Information Systems disciplines together with executives provided different levels of awareness in addressing the questions.

4.0. Evaluation/Analysis of the findings

4.1 How are South African retail banks handling sensitive personal information today?

In all the banks it appears that the answer is *not very well* in terms of international societal expectations. Although, all interviewees did acknowledge the fact that banking is generally considered to be an ethical business and all information that is gathered, stored and disseminated is in the best interests of the customer and that of the bank.

To determine the international societal expectations for handling personal information, previous research, literature and Privacy Laws of overseas countries were assessed. As discussed in Chapter 2, this revealed several areas in which society harbours expectations regarding corporate policies - areas in which advocates, lawmakers, and consumers agree that a reasonable level of policy attention from corporations is appropriate. The areas of concern, viz. improper information collection, new uses of information, sharing information, errors, internal access, and reduced judgement, will be discussed in the following sections. In drawing conclusions regarding approaches to privacy in each of these areas, it is helpful to distinguish between explicit policies, implicit policies and practices.

Explicit policies provide a focal point for the entire organisation and a valid reference for decision making. These policies are well documented and communicated to all staff. Implicit policies are less formal than explicit ones. Implicit policies serve a useful purpose in moving an organisation toward a particular goal, however these may not be as easily communicated, and can be more difficult to enforce. A staff member can always claim ignorance of an implicit policy, but this is difficult to do with a well communicated, explicit policy. In some banks it was found that neither explicit nor implicit policies exist and in these cases, practices are still evident. A summary of the approaches taken by the banks is presented in Table 3.

Table 3 - Corporate Policies

Area of concern	Bank A	Bank B	Bank C	Bank D
Collection	N	N	N	N
New use	N	N	N	N
Sharing	I	I	I	E
Deliberate errors	E	E	E	E
Accidental errors	I	I	I	I
Improper access - computerised	E	E	E	E
Improper access - printout or verbal	I	I	I	I
Reduced judgement	N	N	N	N

In the above table, N = none; I = implicit ; E = Explicit

Each of the areas of concern will now be considered in some detail.

4.1.1 Improper information collection

This area of concern refers to the collection of information with consideration to the principle of the individual's privacy and seek to minimise the data collected. Information held and used for the purpose for which it was originally collected does not pose a problem. Such use is *reasonable* as long as the information is relevant input to a valid decision process. Secretive information collection techniques would be inappropriate for inclusion in such decision making process and can be viewed as *unreasonable*.

All the interviewee's stated that they were not aware of pieces of information available about individuals that the bank refused to store. It appears that the banks do not have a policy to state that *"we do not collect the following information as a matter of policy"*. Two executives (from Bank A and Bank C) indicated that there is information, such as customer buying patterns and other information about customers that will add value in marketing decision making, that their banks do not store. This is due to the perceived excessive demands on disk storage space and the related expense. This type of resistance normally came from the IT department. Common to all banks are plans to collect even more information about their customers. This is highly due to the creation of centralised Customer Information Files, new Database Marketing trends and Data Warehousing concepts. Another executive from Bank C mentioned that there is currently a debate going on within their bank as to whether the race and home language of clients should be stored in the company's files or not. But this issue is still in the argument phase. Despite the new objectives and techniques, the banks had no policy statements regarding the privacy implications of this additional collection of information.

4.1.2 Information used for a new purpose

An area of concern, in which privacy attention is expected, is information held by one entity but used for a purpose other than that for which it was originally collected from the individual. This concern had received no policy attention at the banks. The banks' new approach to targeted marketing entailed even greater collection and uses of customer data. Most of the banks are of the opinion that the use of information in this fashion is in the best interests of the customers and of the bank. Most of the interviewees believe that this is genuinely the case in reality although none of the banks concerned did any market survey or consulted it's clients on an individual basis in this regard. One executive from Bank D mentioned that their bank runs regular focus group meetings with some of their clients and that the issue of privacy was never raised by any client. The following are some of the responses received from the interviewees:

"Although there is no policy in place, this information is used to supply added value to the client and to add to the value-chain from the client's perspective" (Bank D)

"We have a responsibility to inform clients of new product developments and to give the client added value" (Bank B)

"Bad risk client information is made available to credit bureaus via a court or judgement as a legal requirement" (Bank B)

4.1.3. Information shared in new ways across entities

Another area of concern relates to entities sharing personal information in new ways. This area of concern received a great amount of attention by all the banks. In one case the issue had been explicitly addressed and in others the concern was implicitly addressed. Bank D, had explicit policies in place as it uses a computer bureau to handle all its information technology requirements. All the banks have developed a set of policies for sharing customer information with selected third parties. These third parties are selected on the basis that they have a product that will be of some benefit to the bank's client base and any communication to the clients will be under the guidance of the bank. Some third parties were refused permission to do joint mailings with the banks even though they were prepared to pay for the banks' client lists. Strict agreements were required with third parties. These third parties do not pay for the use of the banks client's data. Those banks that had implicit policies regarding the sharing of information with outside parties all stated that *"as a rule we do not sell our client information"*. These banks undertake endorsed mailings to clients so that products and services of third parties are offered to clients only if there is a definite benefit for the targeted clients (in the opinion of the bank) and all production and mailing is conducted by the bank itself. This motivation for the banks actions was in place for a long time even before the issue of privacy became a concern. The banks were at the time concerned with the strategic value of their client information.

4.1.4. Errors

Privacy legislation in Europe, the UK and USA, and societal expectations require that entities guard against errors in handling personal information irrespective of whether these are deliberate or accidental errors.

4.1.5. Deliberate errors

These errors are referred to those errors such as the intentional misreporting of information. All the banks have policies in place in the form of information systems requirements and specifications. There are very stringent balancing controls built into existing systems for most financial information. Also, audits are carried out on a regular basis by internal as well as external auditors. Other errors are normally picked up by administrative controls.

4.1.6. Accidental errors

These are errors such as inaccurate data capture of personal information The errors often go undetected and uncorrected. These errors are not intentional. Here too, it was found that to a certain extent safeguards are built into the systems and processes. Incorrect accidental errors are often encountered as a result of receiving returned mail - these errors are then corrected by various processes that have been created for the recapturing of corrected information. Audit control procedures were also in place to identify some of these errors. Although no explicit policies existed to address these errors, different processes and practices are conducted to rectify these errors.

4.1.7. Improper Access - computerised

Improper internal access to computerised information is another area of concern. Who within the organisation is allowed to access and change personal information in the files? It is often held that individuals should have a *need to know* before access to personal information is granted.

Policies regarding improper access to computerised information are explicitly formulated at all banks, even if these policies were outdated as these are normal banking policies and procedures are in place as to who has what access to data. Banks have computer safeguards to ensure that only authorised individuals can access specific records. Forms for securing access rights are common and policies are documented

4.1.8. Improper Access - printout or verbal

In all banks, access controls for hardcopy printouts and verbal information are not documented in any depth. Although, all banks reported that they have rules as to which printouts need to be filed in safes and which printouts have to be shredded after use. With regard to verbal information, all banks have a confidentiality of information contract that is signed by all staff members. This contract states that all information that the staff member has access to, is confidential and remains the property of the bank. All interviewees were of the opinion that although no explicit policies exist with regard to access control of hardcopy printouts and verbal information, these policies are implicit in the rules that they comply with.

4.1.9. Reduced judgement

An area of concern to international privacy advocates and society is the problem of reduced judgement. This is when the computer is allowed to make decisions on behalf of the decision maker. Expert systems used in Artificial Intelligence based systems are normally used to make such decisions. Two of the interviewees indicated that their banks are currently investigating the use of expert systems but none of the banks have any policies in place regarding reduced judgement.

4.1.10. Summary : Sensitive information handling

Based on the findings, it can be concluded that there is a perceived hierarchy in terms of certain sensitive information practices. The formality of policies was higher for the sharing of information issues than for the collection and new use issues (refer to Table 3). Similarly, policies regarding deliberate errors were more explicit than those regarding accidental errors. There are explicit policies in place for improper access to computerised information and only implicit policies for improper access to printed hardcopy or verbal information. There were no polices in place regarding the issue of reduced judgement.

4.2 How are South African retail banks crafting the policies and practices that govern the use of sensitive personal information?

Generally, it was found that none of the banks have policies that explicitly address the issue of data privacy. This is highly due to the fact that there is no legislation in South Africa to this effect. Also, there has been no consumer backlash or any external threat with regard to this issue. No apparent information privacy policymaking cycle was evident at any of the banks. The banks, due to the nature of their business, have practices in place that could be formalised into actual information privacy policies.

Two of the banks have had their legal departments investigate their vulnerability to the current legislation and there was no problem identified. The banks all seem to adopt a *wait and see* attitude. All the interviewees indicated that they were aware of and agreed that information privacy is of concern both to the bank and their clients. The information privacy policymaking cycle at three banks were consistent in that all information handling practices are controlled by middle level managers. The senior executives of the banks left the responsibility regarding information privacy policies and practices to the middle level managers who implement their own practices based on their own needs. During this period if some practice did not work, it was modified accordingly. These practices will continue to be executed, in what is referred to as a state of *drift* (Smith, 1994), as shown in Table 4, until the banks encounter some sort of external threat e.g. a legislative policy. It is likely that only at this stage that the senior executive/directors of the bank will react and get involved with a decision such as this nature. The policy making cycle is a process whereby the bank is in some area of drift until some external threat is perceived or encountered, after which the bank's executives react to the external threat.

Table 4 - Policy making cycle

Bank	Areas of drift	External threat	Reaction
Bank A	- Customer data used in targeted marketing - Purchasing data about customers - Access to customer data	None	None
Bank B	- Customer data used in targeted marketing - Purchasing data about customers - Access to customer data	None	None
Bank C	- Customer data used in targeted marketing - Purchasing data about customers - Access to customer data	None	None
Bank D	- Customer data used in targeted marketing - Purchasing data about customers - Access to customer data	Competitive	Changes in data use & policies

These banks are involved in targeted marketing activities and have received complaints from clients with regard to incorrect details, but not specific to information privacy. One of these banks, Bank B, submits a computer magnetic tape of its client's name and address details to an outside computer bureau. This bureau would manipulate this client list prior to mailing to the clients

Managers at these banks were not too perturbed with information privacy policies as they felt that banks have always considered information of their customers to be private. Many of these managers have no problem with the international privacy policies. One executive stated that "we have no problem with the policies, except it may cause logistic problems" in reference to the policy of first obtaining the potential respondents permission prior to using the respondent's details. This statement was reiterated by most of the interviewees. Most of the managers were very positive about privacy and three managers said "it is a constitutional right of every single client".

Bank D, as can be seen in Table 4, went through a state of *drift* (where middle level managers crafted their own practices) for some time until the bank perceived an external threat in the form of negative publicity because the systems and controls were not in place and the bank was not aware of the impact of this. Clients were leaving the bank rapidly and the bank obtained a lot of bad debts. The questioning process began by top management and with a new management team in place, started conducting research with their clients as to what the clients wanted. This was done in the form of holding regular focus group meetings with various clients under the guidance of external consultants. The clients were ask what information they were agreeable to give to the bank. The bank explained the different situations when they would use the information to target the clients and received very little or no resistance from the clients. The IS community within the bank, that in the past was opposed to making systems changes without a valid business case or need, fully supported the decisions taken. All the information systems were rewritten in a flexible manner to allow for quick changes taking the new information policy issues into consideration. It should be noted that the reaction to the external threat perceived by Bank D was not devoted to information privacy only. The reaction addresses many issues and information privacy was covered as one of the issues.

4.2.1. Cyclical Policymaking

As is summarised in Table 4, a portion of the drift - external threat - reaction cycle was observed in Bank D. The other banks were still in a state of drift as they have not yet perceived an external threat. Also, most of the interviewees did suggest that if the information privacy policies are legislated, then only will they put policies in place to conform. Until the executives in Bank D perceived an external threat, they allowed the organisation to continue under the direction of middle-to-senior manager's practices as is currently happening in the other banks. The executives attention was devoted to information privacy in a reactive manner as a response to the external threat. This led to emotional dissonance in some of the banks (almost 50 percent of the total number of interviewees), as shown in Table 5 below, and no leadership with regard to information privacy. An interview was considered to have emotional dissonance if the interviewee indicated that he had personal feelings regarding information collection, use, or protection that differed from his or her corporate approach and that these feelings caused the interviewee some concern.

Table 5 - Emotional Dissonance

Bank	Total Interviews	Interviews where emotional dissonance referenced
Bank A	3	2
Bank B	3	1
Bank C	2	1
Bank D	3	1

4.2.2. Emotional Dissonance

Because there are no explicit policies regarding information privacy at the banks, some employees experienced value conflicts regarding their bank's information handling approaches. Some interviewees did not agree with their banks value system when compared with their personal concerns. This was especially predominant with those interviewees working in the marketing discipline (unlike Smith (1993) who found this to be predominant with managers in the IS ranks). This is probably because the IS community believes that there are sufficient policies within all system specifications that the marketing people are not aware of. One marketing executive expressed his concern with the executives of his bank as "*they only pay lip service to privacy issues*".

Other interviewees believed that the privacy policies are practised within their companies even though there are no explicit policies in place. These managers also felt that some of their clients welcomed the idea of receiving mail from the bank as it kept them informed as to new product developments and offerings. The following were some of the responses received from the interviewees:

"*The lower end of our markets do not mind but the concerns with regard to the upper end is fussy. The lower end of the market see this as an opportunity to learn more about the bank and it's products*".

"*Privacy is not an issue to us as we have had no complaints from our customers as yet*".

"*In general, banks are probably one of the most honourable industries where data privacy is held in high stead. Although there are no explicit policies in place, these policies are implicit in the nature of our business*".

4.2.3. IS concerns

It was highlighted in Chapter 2 that while privacy is clearly a strategic issue for organisations, it should be a priority for information systems management as well. As a company's information steward with a broad view of the business, the chief information officer should be in the best position to help his or her firm avoid the crises faced by companies with regard to information privacy issues. While concerns about the use of personal information were raised by some interviewees, these were not really pronounced by the IS community. Many IS people felt that this should be a business initiative. When questioned about the privacy problem, one IS executive brushed it off by saying that it was a marketing function problem even though the IS people provide the expertise with regard to computer-matching processes, database marketing and the simple extraction of customer data. Another IS executive mentioned

"We have built systems with information protection and security of data in mind. Now that these systems and the access to data have been decentralised and control has passed onto the business divisions, these business divisions need to determine what information privacy policies to include as they understand their business better. The business divisions are the owners of the systems and the information. They make decisions as to how it is used. Should the businesses see a gap, we will build the necessary updates to the systems".

Another IS executive said that

"we will play a role as a convenor of discussions around the topic and will be the implementor of the policies, but we do not make the policies".

One interviewee from the marketing discipline, felt that the IS people need to emphasise the privacy issues in the bank. He said

"If this goes into a debate between the marketing and IS people, the IS people will surely win as they have the power to change the systems and put policies in place".

Although the IS community do not run the banks, much of the responsibility for information privacy rests with IS management as they must become acutely aware of potential legal liabilities and how their organisations can best be protected from such risks. This has also been detailed in Chapter 2. It has been suggested that IS managers have and will continue to have oversight responsibility for information liability as they should advise on the confidentiality and security of information.

4.2.4. Leadership roles

Most of the interviewees wanted to adopt privacy policies only after there was some clear guideline by legislation or within the banking industry. Only two of the interviewees indicated a desire to have their company be viewed as a leader in privacy issues. One said

"Why be a leader if there is no concern from our client base. We will, however, do some market research and if it is of concern to our clients then we will lead otherwise we will follow others in the industry".

Another manager, when asked about the feelings from his executive regarding privacy and taking a leadership role mentioned

"The executive do not need to get involved in that level of detail. They would ask us to get it fixed and then tell them. I have no comment about whether we would want to be leaders in this field or not".

Most executives were comfortable in having their banks follow the lead of others, but only a couple of them want their banks to be at the forefront. The executives need not get involved in the details of information privacy, but it seems that they did not understand, according to some interviewees, that information privacy policies and practices could be used to their strategic advantage.

4.2.5. Implications

The implications of the unstructured policymaking process including emotional dissonance and a lack of industry leadership all have negative implications for the effective management of information privacy issues. The most serious implications of this unstructured process is that it leads to gaps between privacy policies and actual current practices. These findings were similar to those of Smith (1993) who found:

- non-existent policies in many important areas;

- gaps between policy and practice;
- leadership vacuums on privacy issues; and
- a corporate climate that inhibits discussions of privacy concerns;

until an external threat is perceived.

It was also revealed that most of the executives are not eager to confront the issue of information privacy. Some of the executives went to some length to avoid the research's discussion and investigation. When these executives confront the issue, it will be in a reactive and not proactive manner, primarily because the decision making process is a cyclical one. It seems that the executives are deliberately avoiding confronting the issue of information privacy for as long as possible. The executives are adopting a wait-and-see attitude and will react on whatever legislation requires them to do.

4.2.6 Summary of findings

The responses to some questions posed to interviewees are summarised in Table 6 below.

Table 6 - Information handling policies

Key questions posed	**Bank A**	**Bank B**	**Bank C**	**Bank D**
Concern for Information privacy?	Y	Y	Y	Y
Conducted studies of probable consumer reaction?	N	N	N	Y
Information systems community involved in policy-making decisions?	Y	Y	Y	N
Tension between personal privacy and information needs	N	N	N	N
Senior executives/directors concern about information privacy?	N	N	N	Y

In the above table, Y = Yes ; N = no.

All interviewees mentioned that information privacy is of concern to them personally although some of the remarks that a few of the participants made were not in line with their comments. Only Bank D has conducted studies of probable consumer reaction even though the main objective of these studies were part of an interactive focus group of existing customers. Similarly, only Bank D did not get their information systems community involved when making policy decision as they have outsourced their information technology department in its entirety. At all banks there was no evidence of tension between personal privacy and information needs. Senior executives were not showing any real concern for information privacy except in Bank D.

5.0 Summary and conclusions

The findings in this research were very similar to that found in research done by Smith (1993), for banks in the United States of America. The results indicate that the banks lack comprehensive policies regulating the access to and distribution of personal data. Banks are generally not willing to become leaders in developing such policies, instead they formulate guidelines and practices only after experiencing some form of external threat. The banks are also not meeting international societal expectations regarding information privacy.

Privacy is an important issue. We know and understand little about what type of information use is appropriate (e.g. telemarketing and direct mail) and what is perceived as an invasion of privacy. Concerns raised by some interviewees suggest that changes with regard to the privacy domain are appropriate and necessary. An interesting finding was the sensitivity of the topic as some executives were often unwilling to discuss their own banks policies and practices.

Executives in South African retail banks are not taking a proactive stance in creating information privacy policies in this ambiguous environment. They are waiting for some external event such as a threat of legislative action to force them to act. Even for other organisations that have these practices in place, privacy helps enforce these standards. This study should be of use to information technology and direct marketing practitioners who are involved with the identification and solution of some of the problems that will be presented by data privacy legislation.

Concerns about privacy are significant and as detailed in Chapter 2, it is something that IT managers and their companies need to deal with sooner rather than later.

5.1 Limitations and Assumptions

This study was exploratory and was limited to doing research at a few South African banks due to time and scope of the study constraints. Although there are many banks in South Africa, it is assumed that the banks chosen are a representative sample as most banks have similar policies and procedures. The difficulty of gaining access to some of the banks initially made the use of personal contacts very important and therefore the banks were not randomly selected. The interviews were targeted at people working in the retail banking environment (this study did not consider merchant and commercial banking)

There is much ambiguity in the information privacy domain internationally. Whether or not there is a right to privacy, which behaviours are appropriate or inappropriate, and how much responsibility corporations should bear, all contribute to the ambiguity.

The research with regard to the sensitive information handling policies served as a *snapshot* of what is currently happening in the banks. What may probably change is that all banks will formalise their information handling policies and practices once this is legislated.

5.2 Management Guidelines

The study shows that management need to adopt a proactive stance towards information privacy and the secondary use of information in total as this will be enforced due to the threat of negative publicity and enforcement through possible legislation. The areas as identified (in Table 3) need attention in areas where policies do not exist or are implicit. An audit of existing processes and procedures is recommended in order to identify possible gaps that may exist. Areas were gaps are identified (as in Table 3) could be used as a point of departure for the questioning process. Once a policy is in place, an education programme needs to be developed to ensure that employees adhere to new policies.

As the company's information providers, the information systems management should understand the implications of the secondary use of information and help their firm avoid the crises faced by some overseas companies with regard to information privacy issues. Some of the appropriate business policies identified can be implemented voluntarily to address public concerns about specific information practices that may be considered a threat to information privacy. The general international privacy needs of individuals need to be integrated with the increased information demands of complex organisations.

5.3 Opportunities/Implications for further research

It is also hoped that increased study of the issue of information privacy from a broader perspective will enhance the probability that the privacy needs of individuals will be integrated with the increased information demands of complex organisations. Research should be conducted to assess and focus on the collection, use and storage of personal information.

In addition to the interviews conducted at banks in this study, interviews need to be conducted in more industries and a written survey questionnaire could be distributed to a sample of employees from each of the industries to assess the gaps between policies and practices with regard to the secondary use of information across the various industries.

What stands out in this study is that the bank executives all have their own opinions about what is best for their clients. Researching the views of the bank's clients will help identify and assess possible gaps between the clients view and the bank executives perceptions.

6. REFERENCE LIST

Agranoff MH, Controlling the Threat to Personal Privacy, *Journal of Information Systems Management*, Summer 1991, pp 48 - 52.

Bloom PN, Milne GR and Adler R., Avoiding Misuse of New Information Technologies. Legal and Societal Considerations, *Journal of Marketing*, Vol. 58, January 1994, pp 98-110.

Burns WJ and McFarlan FW, Information Technology Puts Power In Control Systems, *Harvard Business Review*, September-October 1987, pp 89 - 94.

Burrows B, The Power of Information: Developing the Knowledge Based Organisation, *Long Range Planning*, 1994, Vol. 27, No. 1, pp 142 - 153.

Canning RG, Six Top Information Systems Issues, *EDP Analyzer*, January 1985, Vol. 23, No. 1, Canning Publications Inc., MA, pp 1 - 16.

Canning RG, Information Security And Privacy, *EDP Analyzer*, February 1986, Vol. 24, No. 2, Canning Publications Inc., MA, pp 1 - 14.

Cappel JJ, Closing the E-Mail Privacy Gap, *Journal of Systems Management*, December 1993, pp 6 - 11.

Cespedes FV and Smith HJ, Database Marketing: New Rules for Policy and Practice, *Sloan Management Review*, Summer 1993, pp 7 - 22.

Culnan MJ, Designing Information Systems To Support Customer Feedback: An Organisational Message System Perspective, *Communications of the ACM*, August 1989, pp 305 - 313.

Culnan MJ, "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use, *MIS Quarterly*, September 1993, pp 341 -363.

Dentino K, Taking Privacy into our own hands, *Direct Marketing*, September 1994, pp 38 - 72.

Easterby-Smith M, Thorpe R and Lowe A, *Management Research: An Introduction*, Sage Publications, 1993, London, UK.

Fletcher K, Wheeler C and Wright J, Strategic Implementation of Database Marketing: Problems and Pitfalls, *Long Range Planning*, Vol. 27, No. 1, 1994, pp 133-141.

Gattiker UE, Direct Marketing and Computers: Managing Ethical, Competitive and Privacy Issues, Seminar Handout that was presented for the *South African Direct Marketing Association Seminar*, Johannesburg, 5 May 1995 (a).

Gattiker U, Research Program on Privacy, Caller-ID, Direct Marketing and the Information Highway, article downloaded from the Internet, web site cetus.mngt.uleth.ca, February 1995 (b).

Goodwin C, Privacy Recognition of a Consumer Right, *Journal of Public Policy and Marketing*, Vol. 10 (1), Spring 1991, pp 149-166.

Grupe FH, Commercializing Public Information: A Critical Issue For Governmental IS Professionals, *Information and Management*, 28 (1995), pp 229 - 241.

Hughes G cited by Mazlin D and Jamieson R, An overview of Data Protection in Australia, *Melbourne University Law Review*, Vol. 18, June 1991, pp 83.

Katz JE and Tassone AR, Public Opinion Trends: Privacy and Information Technology, *Public Opinion Quarterly*, Spring 1990, pp 125-143

Kearney RE, Keep Your Hands Off My Data, *Bank Marketing*, May 1995, pp 19 - 22.

Kusscrow RP, The Government Needs Computer Matching To Root Out Waste And Fraud, *Communications of the ACM*, June 1984, pp 542 - 545.

Mason RO, Four Ethical Issues of the Information Age, *MIS Quarterly*, March 1986, pp 5 - 12.

Mazlin D and Jamieson R, Data Privacy and Computer Information Systems, Paper presented at the *Association for Information Systems Americas Conference on Information Systems*, 1994.

McNurling BC, Information And The Law, *I/S Analyzer*, January 1988, Vol. 26, No. 1, United Communications Group, Maryland, pp 1 - 14.

Milne GR, Bloom PN and Adler R, Identifying The Legal and Ethical Risks and Costs of using New Information Technologies to Support Marketing Programs, Edited by Blattberg R, Glazer R and Little JD, The Marketing Information Revolution, 1994, *Harvard Business School Press*, pp 289 - 304.

Neuman PG, *Expectations of Security and Privacy*, Communications of the ACM, September 1994, Vol. 37, No 9, pp 138.

Page TL, The Impact Of Computers on Privacy, *IS Audit and Control Journal*, Volume III, 1994, pp 33 - 39.

Porter ME and Millar VE, How Information Gives You Competitive Advantage, *Harvard Business Review*, July-August 1985, pp 149 - 160.

Remenyi D, So You Want to be an Academic Researcher!, Seminar Handout that was presented for the *Research Methodologies Seminar*, Johannesburg, 4 August 1995.

Rotenberg M, Communications Privacy: Implications for Network Design, *Communications of the ACM*, August 1993, Vol. 36, No. 8, pp 61 - 68.

Rotenberg M, EPIC Program, *EPIC Mailhandler*, Electronic Privacy Information Centre, Washington, USA, February 1995.

Seymo[illegible] T PCs and Privacy Issues, *PC Magazine*, August 1991, pp 89 - 90.

Schwartz EI, The Rush to Keep Mum, *Business Week*, June 8 1992, pp 36 - 38.

Shattuck J, Computer Matching Is A Serious Threat To Individual Rights, *Communications of the ACM*, June 1984, pp 538 - 541.

Smith HJ, Privacy Policies and Practices: Inside the Organizational Maze, *Communications of the ACM*, December 1993, Vol. 36, No 12, pp 105 - 122.

Smith HJ, Information Technology and Corporate America, *University of North Carolina* Press, 1994.

Straub Jr. DW and Collins RW, Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy, *MIS Quarterly*, June 1990, pp 143 - 156.

Tuerkheimer FM, The Underpinnings of Privacy Protection, *Communications of the ACM*, August 1993, Vol. 36, No 8, pp 69 - 73.

Vid'nar N and Flaherty DH, Concern for Personal Privacy in an Electronic Age, *Journal of Communications*, Spring 1985, pp 91 - 103.

White JR, President's Letter ACM Speaks Out, *Communications of the ACM*, May 1991, Vol. 34 No 5, pp 15-16.

Woodman RW, Ganster DC, Adams J, McCuddy MK, Tolchinsky PD and Fromkin H, A Survey of Employee Perceptions of Privacy in Organisations, *Academy of Management Journal*, 1982, Vol. 25, No 3, pp 647 - 663.

7.0 Appendix A

Research questions used in the interview schedule:

7.1. How are South African retail banks handling sensitive personal information today?

Purpose: To help identify the level of concern that banks have regarding information privacy. To establish how well the current banks policies and practices are meeting international societal expectations with respect to uses of personal information.

a) What personal information regarding individuals is stored in the company's files? What is this information used for?

b) Is there related personal information that could be stored in the files but that the bank refuses to store? If yes, what types of information?

c) Who can access and change personal information in the files?
How is this matter decided?

d) Is the information used for any other purposes? If yes, what purposes?

e) Is information shared with other internal and/or external entities
If yes, in what form is this shared and under what conditions?

f) What are the policies for handling accidental errors in the information (e.g. data entry mistakes, mistaken identities, improper ıustering of information)?
What are the safeguards against deliberate errors (intentional misreporting of information, unauthorised changes)?

g) What are the policies, if any, regarding the judgmental processes that must be applied to the use of this information?

h) What are the policies, if any, regarding the combining of several pieces of information into one larger record?

i) How do the executives compare their policies and practices with those of others in the banking industry?

j) Do the operating units' practices conform to these policies?

7.2. How are South African retail banks crafting the policies and practices that govern the use of sensitive personal information?

Purpose: To evaluate the process through which information privacy policies and practices are created in these banks in comparison to international policies and practices.

a) What were the bank's historical positions regarding the use of the information?
When were changes considered, if at all?
How did that questioning process begin: by whom? In what form?
Were there key events that led to the bank to think about how the information was used?

b) What were the trade-offs, if any, in the decisions taken?

c) What arguments, if any, were used in reaching decisions?

d) Where any task forces or the like formed for the questioning process?

e) Were studies conducted of probable consumer reaction to any new policy?

f) Was the IS community involved in the decision-making process?
Did the IS executives instigate any stakeholder analyses?
How did this effort compare with those other executives - e.g. marketing executives?

g) How was the decision-making process ultimately concluded?

h) If the decision represented change, how was it announced and codified?

i) What were the apparent management attitudes toward the tension between personal privacy and information needs?

j) How did the executives feel about potential challenges from privacy advocates?