



COPYRIGHT NOTICE

Please note:

The material contained in this document can be used **ONLY** for **personal** study/research and therefore can be copied but only for **personal** use.

Any form of copying for distribution purposes requires copyright permission from author/university.

INFORMATION PRIVACY RIGHTS OF THE INDIVIDUAL

VERSUS

THE PUBLIC'S RIGHT TO FREEDOM OF INFORMATION

BY

PREGALA PILLAY

DISSERTATION

Submitted in fulfilment of the requirements
for the degree of Magister Administrationis
in the Department of Public Administration
in the Faculty of Commerce and Administration
at the University of Durban-Westville

SUPERVISOR: PROF D SING

JOINT-SUPERVISOR: Dr M S BAYAT

DATE SUBMITTED: JANUARY 1995

DEDICATED TO MY LOVING PARENTS

"I HAVE A DREAM"

I have a dream that one day this nation will rise up and live out the true meaning of its creed: "We hold these truths to be self evident; that all men are created equal".

I have a dream that one day on the red hills of Georgia the sons of former slaves and the sons of former slaveowners will be able to sit down together at the table of brotherhood.

I have a dream that one day even the state of Mississippi, a desert state sweltering with the heat of injustice and oppression, will be transformed into an oasis of freedom and justice.

I have a dream that my four little children will one day live in a nation where they will not be judged by the color of their skin but the content of their character.

I have a dream today.

I have a dream that one day the state of Alabama, whose governor's lip are presently dripping with the words of interposition and nullification, will be transformed into a situation where little black boys and black girls will be able to join hands with little white boys and white girls and walk together as sisters and brothers.

I have a dream today.

I have a dream that one day every valley shall be exalted, every hill and mountain shall be made low, the rough places will be made plain, and the crooked places will be made straight, and the glory of the Lord shall be revealed, and all flesh shall see it together.

This is our hope. This is the faith with which I return to the South. With this faith we will be able to hew out of the mountain of despair a stone of hope. With this faith we will be able to transform the jangling discords of our nation into a beautiful symphony of brotherhood. With this faith we will be able to work together, to pray together, to struggle together, to go to jail together, to stand up for freedom together, knowing that we will be free one day ...

When we let freedom ring, when we let it ring from every village and every hamlet, from every state and every city, we will be able to speed up that day when all of God's children, black men and white men, Jews and Gentiles, Protestants and Catholics, will be able to join hands and sing in the words of the old Negro spiritual, **"Free at last ! Free at last ! Thank God Almighty, We are free at last !"**

MARTIN LUTHER KING JR

ACKNOWLEDGEMENTS

A project of this nature is bound to drain one's energy and intellect as it involves a great deal of thorough research and understanding. In the end it is worth all the effort I have put into it because I have gained tremendous insight and personal growth.

First and foremost, I praise God Almighty, the Supreme Being, who ultimately makes everything possible on earth, for the grace, strength and wisdom to complete this research.

To my supervisor, Professor D Sing, I am forever indebted for the meticulous yet expeditious manner in which he supervised this study. I have drawn much guidance, assistance and encouragement from him.

I am deeply grateful to Dr M S Bayat, my mentor and guide, who encouraged and steered the timely completion of this study. His positive counsel and support were indeed an inspiration to me.

I would be gravely remiss in failing to acknowledge with thanks, the assistance, encouragement and goodwill of the people mentioned below:

The librarians at the University of Durban-Westville and University of Natal, whose research assistance aided my efforts immeasurably;

All the respondents of the questionnaire throughout the country, for their sincerity, and willingness to respond;

Mr Strini Pillay, Ms Romilla Pillay, Mr Roy Reddy, and students at Technikon Mangosuthu for their valued assistance;

Ms S Brijball for her painstaking effort in assisting with the drafting of the questionnaire and the presentation of analysis;

Lecturers in the Department of Public Administration at the University of Durban-Westville and Technikon Mangosuthu, for their academic insight and skill;

A word of thanks to Saveshni Devindran and Inderasan Naidoo, whose willing assistance was crucial to the timeous completion and submission of this study;

Special thanks are also extended to the University of Durban-Westville for the financial assistance which made possible the completion of this research;

My sincere appreciation also goes to my close friends, who are too numerous to mention, for their unfailing encouragement and support;

I am grateful to my parents for their unconditional support, inspiration and abiding love. Thank you for instilling in me the value of education;

To Colin, Kevin, Sandy and Cliffy, I extend my sincere appreciation for the perseverance, motivation and guidance afforded to me during my years of study. I know there will be a sigh of relief now that this is over!!

All those, whom I may have inadvertently missed out, thank you.

P Pillay
Durban
January 1995

D E C L A R A T I O N

I hereby declare that except where acknowledged, this research is entirely my own work, that all sources used or quoted have been acknowledged and that this dissertation has not previously been submitted for a degree or diploma at another tertiary educational institution.

Pregala Pillay
January 1995

TABLE OF CONTENTS

	PAGE
CHAPTER ONE	
RESEARCH METHODOLOGY AND ORGANISING OF CHAPTERS	
1.1	Introduction 1
1.2	Research Methodology 3
1.2.1	Theory Search and Case Analysis 5
1.2.2	Empirical Survey and Data Interpretation 6
1.3	Limitations of Study 6
1.4	Overview of Chapters 7
1.5	Definition and Terminology 12
1.5.1	Information Privacy 12
1.5.2	Freedom of Information 13
CHAPTER TWO	
INFORMATION PRIVACY	
2.1	Introduction 14
2.2	Relationship between the State and the Individual 17
2.3	Privacy 20
2.3.1	Private and Public Differentiated 20
2.3.2	Definition of Privacy 22
2.3.3	Right to Privacy 24
2.3.4	Need for Privacy 27
2.3.5	Desire for Privacy 28
2.4	Personal Information 31

2.4.1	Defining the term "Personal"	31
2.4.2	Defining the term "Information"	33
2.4.3	Defining the concept "Personal Information"	34
2.5	Definition of Information Privacy	35
2.5.1	Threat to Information Privacy	36
2.5.2	State's Role in Information Privacy Protection	39
2.5.2.1	Features of a National Policy	40
2.5.2.2	Objectives of a National Policy	41
2.6	Summary	43

CHAPTER THREE

TECHNOLOGICAL CHANGE - COMPUTER REVOLUTION

3.1	Introduction	46
3.2	Defining Technology	48
3.2.1	Reasons for the use of Technology	49
3.2.2	Impact of Technological Developments on the Right to Privacy	49
3.2.3	Problems of Privacy in a Technological Age	51
3.3	Computer Technology	52
3.3.1	Purposes of Computers	52
3.3.2	Definition of Computer Technology	53
3.3.3	Advent of the Computer Age	54
3.3.3.1	Computer and its Contemporary Impact on Public Administration	56

3.3.3.2	Computers and the Storage of Information	58
3.3.3.3	Computers and "Provisional Catastrophe"	60
3.3.3.4	Effect of Information in Computers and its Implication for Privacy	61
3.3.3.5	Computer Linkage or Computer Matching	65
3.4	Transborder Data Flows	66
3.4.1	Remedies	67
3.4.1.1	International Instruments	67
3.4.1.2	Transnational Data Protection Principles	69
3.5	Examples Illustrating the Inappropriate, Unauthorized or Illegal Access To and Use of Personal Information	72
3.6	Information Privacy Protection Principles	74
3.7	Safeguards	75
3.8	Summary	79

CHAPTER FOUR

FREEDOM OF INFORMATION

4.1	Introduction	82
4.2	Definition of Freedom of Information	84
4.3	Freedom of Information	84
4.3.1	Disclosure of Government Information	85
4.3.2	Disclosure of Government Information as a Means	87
4.3.3	Criticism of Disclosure of Government Information as a Right	88

4.3.4	Freedom of Information and Accountability	88
4.3.5	Freedom of Information and Public Administration	90
4.3.6	Rationale for Freedom of Information	91
4.3.7	Continuing Struggle over Citizen Access to Government Information	92
4.4	Politics and Secrecy	96
4.4.1	Need for Government Secrecy	97
4.4.2	Cost of Freedom of Information and Secrecy	100
4.5	Democracy and Freedom of Information Legislation	102
4.5.1	Need for Freedom of Information Legislation	103
4.5.2	Exclusions, Enforcements and other Considerations	107
4.5.3	Specific Limitations on Access	107
4.5.4	Publication of Documents by the Government	112
4.5.5	Scope of Public Institutions Covered by the Access Legislation	113
4.6	Summary	114

CHAPTER FIVE

TRENDS IN INFORMATION PRIVACY PROTECTION AND PROMOTION OF FREEDOM OF INFORMATION : INTERNATIONAL AND NATIONAL PERSPECTIVE

5.1	Introduction	116
-----	--------------	-----

5.2	Information Privacy and Freedom of Information Laws	118
5.3	Information Privacy Legislation : International Perspective	119
5.3.1	Federal Republic of Germany	119
5.3.1.1	Appointment of the Federal Data Protection Commissioner	120
5.3.1.2	Duties of the Federal Data Protection Commissioner	121
5.3.1.3	Staff of the Federal Data Protection Commissioner	122
5.3.1.4	Chronology of German Data Protection Legislation	123
5.3.2	Sweden	125
5.3.2.1	Data Inspection Board	125
5.3.2.2	Staff of the Data Inspection Board	125
5.3.2.3	Chronology of Swedish Data Protection Legislation	126
5.3.3	France	129
5.3.3.1	National Commission on Data Processing and Freedoms	129
5.3.3.2	Staff of the National Commission on Data Processing and Freedoms	129
5.3.3.3	Chronology of French Data Protection Legislation	130
5.3.4	United Kingdom	133

5.3.5	Canada	134
5.3.5.1	Privacy Commissioner	134
5.3.5.2	Developments in Canadian Data Protection	135
5.3.5.3	Chronology of Canadian Data Protection Legislation	136
5.3.6	United States of America	138
5.3.6.1	Privacy Act of 1974	138
5.3.6.2	Privacy Protection Study Commission	139
5.3.6.3	Chronology of United States Federal Data Protection Legislation	139
5.4	Information Privacy Legislation : National Perspective	141
5.4.1	South Africa	142
5.4.1.1	Measures to protect Information Privacy Rights	143
5.5	Freedom of Information Legislation : International Perspective	150
5.5.1	United States of America	152
5.5.2	Sweden	155
5.5.3	Australia	157
5.5.4	Canada	158
5.6	Freedom of Information Legislation : National Perspective	160
5.6.1	South Africa : Historical Perspective	160
5.6.1.1	Restrictive South African Legislation	162
5.6.2	Developments in South Africa	163

5.6.2.1	Bill of Fundamental Rights and Constitutional Principles	164
5.6.2.2	Reconstruction and Development Programme	165
5.6.2.3	Recent Developments	166
5.6.3	Principles for a Freedom of Information Law for South Africa	166
5.6.4	Balancing Conflicting Interests	169
5.7	Summary	171

CHAPTER SIX

EMPIRICAL SURVEY OF INFORMATION PRIVACY AND FREEDOM OF INFORMATION

6.1	Introduction	180
6.2	Aim of the Study	180
6.3	Description of Sample	182
6.4	Procedure	183
6.5	Research Instruments	183
6.6	Statistical Analysis of the Data	185
6.6.1	Chi-square Analysis	185
6.6.2	Cumulative Indices	186
6.7	Interpretation of Research Findings	186
6.7.1	Information Privacy	187
6.7.2	Privacy and Computers	202
6.7.3	Privacy and the Future	208
6.7.4	Freedom of Information	217

6.7.5	Freedom of Information and Information Privacy	230
6.8	Summary	232

CHAPTER SEVEN

CONCLUSION AND RECOMMENDATIONS

7.1	Introduction	234
7.2	Recommendations	237
7.3	Summary	245

BIBLIOGRAPHY

1. PUBLISHED SOURCES

1.1	Books	247
1.2	Periodicals and Journals	254
1.3	Dictionaries	255
1.4	Reports	256
1.5	Newspapers	256
1.6	Government Publication	257

2. UNPUBLISHED SOURCES

2.1	Dissertations	257
2.2	Official Documents	257
2.3	Symposiums	258

LIST OF TABLES, PIE CHARTS, BAR CHARTS AND APPENDICES

TABLES

5.1	Chronology of German Data Protection Legislation	124
5.2	Chronology of Swedish Data Protection Legislation	128
5.3	Chronology of French Data Protection Legislation	132
5.4	Chronology of Canadian Data Protection Legislation	137
5.5	Chronology of United States Federal Data Protection Legislation	140
6.1	Collection of Personal and Sensitive Information	190
6.2	Chi-square Table	192
6.3	Chi-square Table	193
6.4	Chi-square Table	194
6.5	Information Available to a Requester	198
6.6	Individuals/Institutions Responsible for Privacy Protection	200
6.7	Privacy Protection by Means of Legislation	209
6.8	Chi-square Table	210
6.9	Chi-square Table	211
6.10	Chi-square Table	212
6.11	Chi-square Table	220
6.12	Chi-square Table	222

6.13	Chi-square Table	222
6.14	Access to Information	224
6.15	Withholding of Certain Information by Government	225

PIE GRAPHS AND BAR GRAPHS

6.1	Graphic representation depicting the Public's Concern about Privacy in South Africa	197
6.2	Graphic representation illustrating the Major Institutions Responsible for Protecting the Privacy of Individuals in South Africa	201
6.3	Graphic representation depicting Legislation Designed by the State to Protect Information Privacy	206
6.4	Graphic representation depicting the Computer as the Major Threat to Information Privacy	207
6.5	Graphic representation depicting the Need for a Privacy Committee to Protect Privacy	213
6.6	Graphic representation depicting the Need for an Independent Authority to Handle Complaints about Violation of Personal Privacy	215
6.7	Graphic representation depicting Government Functioning in Secrecy	219
6.8	Graphic representation depicting a Need for an Open System of Government	221

6.9 Graphic representation depicting the Role of the Courts in Determining Access to Information	229
--	-----

APPENDICES

1. Questionnaire	260
2. Fundamental Rights	277
3. Constitutional Principles	284
4. Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data	288
5. Council of Europe: Extracts from the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	292
6. European Commission: Proposal for a Council Directive concerning the Protection of Individuals in relation to the Processing of Personal Data	298
7. Privacy Committee's Recommended Data Protection Principles	306

**INFORMATION PRIVACY RIGHTS OF THE INDIVIDUAL VERSUS
THE PUBLIC'S RIGHT TO FREEDOM OF INFORMATION**

By

Pregala Pillay

SYNOPSIS

Supervisor:	Prof D Sing
Joint Supervisor:	Dr M S Bayat
Degree:	Magister Administrationis
Faculty:	Commerce and Administration
University:	University of Durban-Westville

In this dissertation a study of information privacy rights of the individual versus the public's right to freedom of information is undertaken.

Information privacy involves the rights of individuals in relation to information about them that is circulating throughout society. The possession of information implies the possession of power and the government increasingly desire information from its citizens in exchange for the basic services and amenities it provides.

The role of the government in the private affairs of the individual has greatly increased. The government simultaneously becomes privy to the personal details of the citizen.

Since government's need for information about citizens has increased, it requires a system to store this information. In addition, public institutions are forced, by the constant search for efficiency, to make use of the best available tools. One such tool is the computer.

Government maintains integrated dossier files on every member of the population by using computer equipment. Information collected for particular purposes may be used to build up a picture of an individual's lifestyle at the push of a button. Decisions affecting an individual's welfare may be based on information that is inaccurate, outdated or irrelevant. In this way the individual becomes unfairly disadvantaged for the benefits provided by government, although no fault of his own. Because the information is given by the computer, it is thought to be objective and infallible.

Essential safeguards are necessary to prevent the misuse and abuse of personal information. These include information privacy protection principles, professional

training and ethics for computer programmers, the appointment of an ombudsman to investigate violations of personal privacy and provisions sanctioned by law to prevent the gross violations of personal privacy.

On the other hand, freedom of information is a contemporary issue in western democracies. It implies the right to publish information and allow the free flow of information without undue government restrictions. Access to information is the citizen's best guarantee that government is conducted in the public interest. It creates a citizenry that is knowledgeable and informed of the matters that ultimately affect them. This state of affairs necessitates the implementation of a Freedom of Information Act.

Whilst access to official information legislation is aimed at protecting the public's right to know, privacy protection legislation is intended to give the individual citizen better control over the collection, storage and dissemination of information by public institutions.

Privacy protection and access to information are fundamental constitutional principles found in many western democracies.

There is an urgent need for information privacy and freedom of information rights in South Africa. This study focuses on both the theoretical and practical aspects of information privacy and freedom of information. These aspects are analyzed in order to provide a foundation for the policy-makers to address the inadequacy of privacy and freedom of information rights in South Africa.

RECOMMENDATIONS:

In the final analysis certain recommendations were made. These include:

- Further research into information privacy and freedom of information must be undertaken;
- A policy for information privacy and freedom of information should be adopted and continually revised;
- Information privacy protection principles should be instituted by all public record keeping authorities;
- An independent authority to handle complaints about the violations of personal privacy must be created;

- The role of the courts in information privacy protection and freedom of information should be highlighted;
- The ombudsman is a vital instrument in enhancing the success of information privacy and freedom of information;
- An educational programme should be designed to acquaint public administrators of the dynamics of information privacy and freedom of information;
- The administration of personal information by public institutions must be effective;
- Legislation on information privacy and freedom of information should be drawn up concurrently; and
- The citizens of South Africa should not allow the government to function in secrecy.

CHAPTER 1

RESEARCH METHODOLOGY AND ORGANISING OF CHAPTERS

Homo sapiens who stood at the dawn of the first material civilisation at the end of the last glacial age, is now standing at the threshold of the second, the information civilisation, after ten thousand years.

Yoneji Masuda (in Sing 1986 : 2)

1.1 INTRODUCTION

Kreimer (1991 : 3) states that modern government has taken progressively greater responsibility for functions that were previously left to the market or other social structures. In the late twentieth century, the bureaucrat, who dispenses benefits and licenses, hires and fires, plans health care programmes or fiscal policy, has replaced the police officer, judge or soldier as the icon of government.

As John Spender (in Sing 1986 : 2) aptly states:

Our right to privacy is under challenge by those who would enchain us for our own good ... By the planners, the zealots and the social engineers for whom efficiency - not liberty, not justice - is the goal.*

* Direct quotations are indented and darkened throughout the course of this research.

In the course of his job, the bureaucrat learns more intimate details about citizens than would the police officer or the judge. This information is stored in computers which have voracious appetites for information, and every license, benefit or exemption makes the government privy to the details of a citizen's life. In this way the government poses a threat to the personal privacy of the citizen, of which he knows nothing (Kreimer 1991 : 3).

Information is the currency of democracy. Madison (in Riley 1986 : 17) stated the case a century and a half ago in the following memorable words:

A popular government without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both. Knowledge will forever govern ignorance: and a people who mean to be their own governors, must arm themselves with the power which knowledge gives.

Freedom of information guarantees to the citizen a right of access to information, albeit with certain conditions. It means that the citizen will be in a position, if he so chooses, to know what one's government is doing and why. It implies further that the citizen, who pays the taxes

which finance the gathering of that information, will have the right to scrutinise the information and there should exist the opportunity for the electorate to be informed. Freedom of information is thus a testament to, and a symbol of open government by a knowledgeable and informed sovereign citizenry (Riley 1986 : 67).

1.2 RESEARCH METHODOLOGY

In the light of the background issues discussed above, the broad research goal of this study was determined through the following objectives:

- (i) To determine the extent to which information has been computerised in South African public institutions;
- (ii) To understand and evaluate the various concepts and principles underlying information privacy and access to information in the international arena;
- (iii) To develop administrative systems through which a balance can be maintained between information privacy protection and public access to information;
- (iv) To propose and devise a model for a general information protection and access to information law

in South Africa; and

- (v) To draw conclusions and make recommendations that may contribute to the implementation of information privacy and freedom of information legislation.

Certain questions were extracted from the literature survey and acknowledgement is made of the questions used by Harris and Westin in their research entitled: **The Dimensions of Privacy: A National Opinion Research Survey toward Privacy, 1981.**

The research findings of the empirical survey were statistically analyzed and reported, and a model on information privacy and freedom of information was devised.

The research intends to answer the following questions:

- (i) What does the term "information" mean in the context of South African public institutions?
- (ii) What criteria should be used to determine which information held by public institutions be confidential and which information be made freely accessible to the public?

- (iii) What principles should be applied to prevent inappropriate, unauthorized or illegal access to and use of information held by public institutions?
- (iv) How can the model for information privacy rights and access to information law be integrated in a Bill of Rights in a new South Africa?

The research consists of the following three aspects:

Theory search and research model construction,
Empirical survey, and
Data interpretation.

These aspects are explained below:

1.2.1 THEORY SEARCH AND CASE ANALYSIS

A literary study of available texts comprising relevant books, journals, dissertations, legislation proposals, and departmental rules and regulations, have been undertaken.

In order to obtain a global perspective of information privacy and freedom of information, a study of various international reviews were made. It was necessary to communicate with various international academics and institutes in order to fully comprehend the developments of information privacy and freedom of information in the

respective countries.

1.2.2 EMPIRICAL SURVEY AND DATA INTERPRETATION

A survey was conducted by distributing questionnaires designed to measure attitudes of high ranking officials namely, senior administrative officials, with reference to information privacy and access to official information.

The data interpretation consisted of the following:

- (i) Determining of relative values pertaining to the established criteria which emerged from the survey, and transferring the coded data onto a computer data base.
- (ii) Developing a situational theoretical model for attitudinal dimensions of senior officials, the components of which have been derived from the literature search and the results of the survey.

1.3 LIMITATIONS OF THE STUDY

It is accepted that in a research undertaking of this nature there will always be limitations. The primary concern is that:

The questionnaires were intended to gather information on information privacy and freedom of information, but were poorly answered by the senior administrative officers. A reason advanced here was that these issues of information privacy and freedom of information were not accorded sufficient attention by the old apartheid regime. It has come to light recently that the public needs a legal right to correct and verify personal records held by public institutions, and a right to official information in the new South Africa. Consequently senior administrative officers lacked knowledge and insight when answering the questionnaire.

1.4 OVERVIEW OF CHAPTERS

The chapters in this study are organised as follows:

CHAPTER 1 : DEMARCATION OF STUDY FIELD AND RESEARCH METHODOLOGY

This chapter demarcates the field of study, and outlines the research methodology. It includes a formulation of the research objectives and study goals, as well as an overview of the proposed study.

CHAPTER 2 : INFORMATION PRIVACY

Many people regard privacy as "the right to be let alone" (Hendricks, Hayden and Novik 1990 : xi). There is no doubt that privacy emerges as one of the central problems of modern times. The problem of privacy involves achieving an appropriate balance between the genuine right to individual privacy, on the one hand, and the equally legitimate need of society to know, on the other. It is because one recognises both the individual's right to privacy and society's need to know that there is a conflict of rights which is at the heart of the problem of privacy in this modern era (Bier 1980 : xi).

This chapter begins with the concept of "privacy" as an individual freedom and value, and endorses a definition of information privacy. It also considers the question of intrusion by government upon an individual's privacy.

CHAPTER 3 : TECHNOLOGICAL CHANGE - COMPUTER REVOLUTION

The growth of technology in today's world can be viewed as an irresistible drive for efficiency, and an urge to achieve the maximum production of goods and services with the minimum of human effort. The increase in the flow of information induced by the computer threatens the individual's ability to control the flow of information

about himself: his privacy is endangered (Rowe 1972 : 13).

Wacks (1989 : 178) asserts that the widespread use of computers facilitates incomparably speedier and more efficient methods of storing, retrieving, and transferring information than is possible with conventional manual filing systems. In the absence of clearly formulated legal controls, there is a serious danger of creating an automated, authoritarian society from which there is no escape.

This chapter is concerned with privacy and technology. It considers the use of computers, the large quantities of information about individuals stored in data banks and the potential danger of misuse by such computer systems.

CHAPTER 4 : FREEDOM OF INFORMATION

Robertson (1982 : 13) is of the view that freedom of information is an essential element of a democratic society. However, all information cannot be made accessible: there is a need to keep legitimate secrets in government. To this end, some confidentiality is required.

What is needed is a new spirit in government - one that recognizes that all talk of participatory democracy is sheer hypocrisy if the public is denied the right to obtain

the information that will allow it to make up its own mind on the issues that ultimately affect it. **To govern is to inform; to be well governed is to be well informed** (Robertson 1982 : 181).

This chapter focuses on the definition of freedom of information, the necessity for freedom of information and public administration, access to public information as a human right, freedom of information and the political process, and the need for government secrecy.

CHAPTER 5 : TRENDS IN INFORMATION PRIVACY PROTECTION AND PROMOTION OF FREEDOM OF INFORMATION: INTERNATIONAL AND NATIONAL PERSPECTIVES

According to Bulmer (1979 : 2) the protection of personal privacy is a complicated issue. Concern for the protection of privacy is one of the most pressing social issues in every western country.

Warner and Stone (1970 : 123) asserts that individuals fear the loss of control over their own personal privacy as an information society continues to evolve. The concern for privacy stems from the computerization and automation of personal information which is proceeding at a pace that George Orwell (author of 1984) could not have anticipated.

Some of the dangers to individual privacy from the operation of data banks are addressed by protection legislation in most western democracies (Sloan 1986 : 10).

Sieghart (1988 : 100) is of the opinion that countries which are acknowledged to be democratic vary in the amount and kind of government information that is available to the public. The degree to which government information is available to the public depends on the type of authority that is elected and the system of government that is followed. An analysis of the various countries will show that the existence of a high or low level of government secrecy is dependent upon the structure of political authority in each country.

The first part of this chapter focuses on the effectiveness of the law as the principal avenue through which information privacy may be protected and preserved. A model is proposed for South Africa.

In the second part of this chapter an attempt is made to analyze the legal system relating to freedom of information in various countries, and to propose a draft legislation for South Africa.

CHAPTER 6 : PRESENTATION AND ANALYSIS OF RESULTS

This chapter focuses on the empirical research and the presentation of such data is compiled.

CHAPTER 7 : CONCLUSION AND RECOMMENDATIONS

Chapter 7 contains general conclusions and recommendations arising from the empirical research.

1.5 DEFINITION AND TERMINOLOGY

It is important for the purposes of this discussion to provide definitions of significant concepts.

1.5.1 INFORMATION PRIVACY

Ware (1979 : 243) defines information privacy as:

The social expectation that an individual:

- will be treated fairly and accurately by information taking systems;
- will be protected against intrusive collection of information; and
- should have a legitimate enforceable expectation that records maintained about him will be treated as

confidential.

5.1.2 FREEDOM OF INFORMATION

According to Riley (1986 : 1) freedom of information means different things to many people.

To those in the media, and to others, it implies the right to publish information and to allow the free flow of information without undue government restrictions. It means the right to inform the public without being fettered by regulations which in any way restrict this right. In another context, it has come to mean the free flow of information across borders unfettered by government regulations.

CHAPTER 2

INFORMATION PRIVACY

Every man must understand for himself what others say or write. The others cannot understand for him. It is his concepts, not theirs, which are operative when he "follows" what his neighbours say.

Price (in Young 1978 : 13)

2.1 INTRODUCTION

The International Social Science Journal (1972 : 418) provides a relevant conceptualization of privacy:

Nearly everyone wants to keep some part of his life, his thoughts, his emotions, his activities private to himself or to chosen members of his family and friends. The extent of this private life, the area of privacy, will vary also according to differing ages, traditions and cultures. But though the area of privacy may vary, the desire for privacy is universal. Until recent times, the private life of the individual was primarily what he did in the intimacy of his home, the walls of his home constituting as it were the boundary between

his public and his private life. Nowadays, the individual is becoming more and more transparent to his fellow-men, even where his private life is concerned.

According to the New South Wales Privacy Committee Report (1983 : 1) there are three types of privacy:

- Territorial Privacy: an individual's interest in having a physical domain within which he can be left in solitude and tranquillity;
- Privacy of the Person: an individual's interest in being protected from physical harassment or subjection to indignity; and
- Information Privacy: an individual's interest in controlling the collection, storage and circulation of information about himself.

This chapter focuses on information privacy, which involves the rights of individuals in relation to information about them that is circulating throughout society.

The importance of information privacy has increased with the advent of the computer age and the information society. One significant reality is that modern life has been transformed from an age when a handful of institutions kept

a few paper records in filing cabinets, into the fast moving present in which many activities are recorded and stored by huge computer systems operated by megacorporations and government institutions (Hendricks et. al 1990 : xi).

Report of the Privacy Protection Study Commission (1977 : 3) reports that one need only refer briefly to the dramatic changes in recent times to understand why the relationship between personal privacy and record keeping has become an issue in almost all modern societies.

Today, government regulates and supports large areas of economic and social life through some of the nation's largest bureaucratic organizations, many of which deal directly with individuals. It is commonplace for an individual to be asked to divulge information about himself for use by unseen strangers who make decisions about him that directly affect his everyday life. Because so many of the services offered by public institutions are considered necessities, an individual has little choice but to submit to whatever demands for information an organization may request from him. This information is used to facilitate finely-tuned decision-making for the individual (Report of the Privacy Protection Study Commission 1977 : 3).

2.2 RELATIONSHIP BETWEEN THE STATE AND THE INDIVIDUAL

There has been a marked tendency on the part of the executive to interpret the public interest more in terms of its own efficiency than in terms of popular control, and a by-product of this tendency has been a growth in executive secrecy.

Williams (in Young 1978 : 87)

The relationship between the State and the individual is a long and lasting one. Man is to be found everywhere, living in some form of association with his fellow men. And where there is association, or society, there is the condition of government: a system to regulate, direct and generally exercise control over at least some of the affairs and activities of the individuals who collectively compose any society. The organization of government may vary from ordered and stable life in the primitive community, to the direction and control of most of man's activities in a manner generally regarded as a feature of the totalitarian regime. The important point is that man only exists as part of society, and that a society, in turn, is the sum of the individuals who compose it (Young 1978 : 87).

Hobbes and Locke (in Young 1978 : 87) asserts that the relationship between the individual (citizen) and the State (government) is in the form of contract, where the individual relinquished absolute control over his own affairs in order to gain the benefits of a social existence.

Rowe (1972 : 22) is of the opinion that man is born into society, without a choice of belonging; and history has shown it is a fiction to believe that liberties preceded government and social control. The notion of a contract does serve the purpose of highlighting an important strand of political thought. As a consequence of sacrificing certain basic rights or liberties and submitting himself to social control, the individual should secure considerable rewards. Furthermore, the individual should impose strict safeguards to preserve his remaining rights. The relationship is thus a balance of obligations, duties and responsibilities on the one hand, and of certain benefits, and liberties on the other.

Miller (1971 : 27) argues that:

The sole end for which mankind are warranted, either collectively or individually, in interfering with the liberty of action of any of their number, is self protection... That the only purpose for which power can

be exercised over any member of a civilised community, against his will, is to prevent harm to others.

He intends to show that man's affairs are his private concern except where they affect the private affairs of others. Only then can they reasonably be considered to have become matters of public concern. The concept of "information privacy" is closely related to this kind of argument since it assumes that there are certain areas of the individual's life which are of a private nature and which should be protected from public intrusion. This "personal area" may consist of personal behaviour, personal thoughts or personal information (Young 1978 : 88).

Martin (1988 : 44) believes that in the field of public administration, the remedies for the privacy issue are much more scarce simply because one can neither remove oneself from the activities of most government departments and authorities nor evade their investigation. There are certainly some departments and authorities in this area to whose activities one need not subscribe, but for the most part, one has no choice. Co-operation, willing or otherwise, with various institutions of government, is an obligation of citizenship.

2.3 PRIVACY

**The grounded maxim so rife and celebrated
in the mouths of wisest men ; that to the
public good private respects must yield...**

John Milton (in Young 1978 : 1)

The concept of "privacy", being essentially a component of freedom, raises immediate difficulties of definition, and even less common agreement about what is desirable. The conflict between the State and the individual is continuous and self-generating. The State's interests are served by the need to know as much about its citizens as possible. There are many times when citizens must give personal information, both for their own and the common good. The argument is about how one can best reconcile the right of the individual to be left alone when society needs to know about him (Madgwick and Smythe 1974 : 1).

Before analyzing the concept of privacy, some attention must be focused on understanding what is "private" and what is "public".

2.3.1 PRIVATE AND PUBLIC DIFFERENTIATED

At the heart of the concern to protect privacy according to Wacks (1989 : 7) lies a conception of the individual and

his or her relationship with society. For the Greeks a life spent in the privacy of "one's own" (idion), outside the world of the common, was by definition idiotic. Similarly, the Romans regarded privacy as merely a temporary refuge from the activities of the res publica. It is only in the late Roman period that it is possible to detect the beginnings of a recognition of privacy as a zone or sphere of intimacy.

As Hanna Arendt (in Wacks 1989 : 7) observes:

In ancient feeling, the privative trait of privacy, indicated in the word itself, was all-important; it meant literally a state of being deprived of something, and even of the highest and most human of man's capacities. A man who lived only a private life, who like the slave was not permitted to enter the public realm, or like the barbarian had chosen not to establish such a realm, was not fully human.

There is a relationship between the existence of the public/private dichotomy and other fundamental features of a society. One such model is the distinctive representation of societies as exhibiting the characteristics of Gemeinschaft (in which there is a community of internalized norms and traditions regulated according to status but mediated by love, duty and a

shared understanding and purpose), or Gesellschaft (where self-interested individuals compete for personal material advantage in a so-called free market). In the former there is virtually no distinction between private and public, while in the latter the division is strongly demarcated (Wacks 1989 : 8).

2.3.2 DEFINITION OF PRIVACY

Privacy means different things to different people. It is an elusive concept, difficult to define. Numerous definitions have been cited in the literature:

One of the earliest scholars to define "privacy" was Louis D Brandeis (in McClellan 1976 : 3) who, in 1890, referred to it as **the right to be let alone.**

Westin (1970 : 7) first described privacy as ... **The state of solitude or small group intimacy.** The second noted definition was that ... **Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.**

Fried (1970 : 138) proposed that privacy provides **the rational context for a number of our most significant ends, such as love, trust and friendship, respect and self**

respect.

According to Ruebhausen and Brim (Columbia Law Review 1965 : 1189) **the essence of privacy is no more, and certainly no less, than the freedom of the individual to pick and choose for himself the time and circumstances under which and most importantly, the extent to which, his attitudes, beliefs, behaviours, and opinions are to be shared with or withheld from others.**

Miller (1971: 25) defines "privacy" as **the individual's ability to control the circulation of information relating to him.**

According to Parker (Rutgers Law Review 1974 : 280) **privacy is control over whom and by whom the various parts of us can be sensed by others ... control over who can see us, hear us, touch us, smell us, and taste us, in sum, control over who can sense us, is the core of the concept of privacy. It is the control over the sort of information found in dossiers and data banks.**

Among the various definitions of privacy which have been presented, a number of distinct elements may be identified: access to oneself, information about the self, respect for the person or for human dignity, autonomy and personal space.

2.3.3 RIGHT TO PRIVACY

The Stockholm Conference (in International Social Science Journal 1972 : 420) defined the "Right to Privacy" as

The right to be let alone to live one's own life with the minimum degree of interference. This means the right of the individual to lead his own life protected against:

- (a) interference with his private, family and home life;
- (b) interference with his physical or mental integrity or his moral or intellectual freedom;
- (c) attacks on his honour and reputation;
- (d) being placed in a false light;
- (e) disclosure of irrelevant embarrassing facts relating to his private life;
- (f) the use of his name, identity or likeness;
- (g) spying, prying, watching and besetting;
- (h) interference with his correspondence;
- (i) misuse of his private communications, written or oral; and
- (j) disclosure of information given or received by him in circumstances of professional confidence.

One aspect of privacy which was not considered in any detail at the Stockholm Conference, but is now considered by many people to constitute, potentially, the greatest threat of all: namely, the collection, storage and dissemination of personal information by means of computers or data banks (International Social Science Journal 1972 : 420).

According to the South African Law Commission (de Villiers, van Vuuren and Wiechers 1992 : 365)

Everyone has the right to the protection of his or her privacy, which means, inter alia., that his or her property or place of residence or employment shall not be entered, that he or she shall not be searched, that his or her property or possessions shall not be seized and that there shall be no interference with or interception of his or her correspondence or other forms of communication.

According to the African National Congress Freedom Charter and Bill of Rights (in de Villiers et. al 1992 : 365) the right to privacy is defined as follows:

No search or entry shall be permitted except for reasonable causes, as prescribed by law, and as would be acceptable in an open and democratic society;

Interference with private communications, spying on persons, and the compilation and keeping of secret files about them without their consent, shall not be permissible as authorised by law in circumstances that would be acceptable in an open and democratic society.

According to Rowe (1972 : 19) a panel on Privacy and Behavioural Research defined the right to privacy as

The right of the individual to decide for himself how much he will share with others his thoughts, his feelings, and the facts of his personal life ... actually what is private varies from day to day and setting to setting.

The National Council for Civil Liberties (1971 : 1) defines the right to privacy as the right to:

- a) solitude, being his right to have his physical senses unmolested in any private place;
- b) intimacy, being his right to enjoy in any private place the close familiarity of his family, work or social group;
- c) anonymity, being his right to prevent undue publicity of himself;

- d) reserve being his right to prevent psychological investigation on his mind or brain; and
- e) privacy of his personal information, being his right to prevent the recording of any information kept by him or by any other person which expressly or by necessary implication refers to him.

Report of the National Council for Civil Liberties Evidence for the Younger Committee on Privacy (1971 : 2) reports that the right to privacy must be balanced by the right to freedom of information, the public's right to know matters of legitimate interest or concern, and freedom of expression. Because the individual's right to privacy includes the right of access to private information held about oneself, freedom of information and freedom of expression complement the right to individual privacy by encouraging open government.

2.3.4 NEED FOR PRIVACY

Man is a social animal. No human being can exist for long in total isolation from all others. There is also a need to withdraw from others, to a greater or lesser extent, at different times of one's life (Sieghart 1976 : 8).

Sieghart (1976 : 8) states that to preserve his sense of identity and the integrity of personality, to work out personal relationships and find a way to personal salvation, each human being needs to be able to limit the area of his intercourse with others. The chosen area will fluctuate from person to person and from movement to movement: there are times when one needs solitude and others when one needs the comfort of one's friends; there are times when one needs the intimacy of communication with one or more people who are close, and times when one needs to maintain one's reserve. Above all one needs to be able to keep to oneself those thoughts and feelings, beliefs and doubts, hopes, plans, fears and fantasies, which one calls "private", precisely because one wishes to be able to choose freely with whom and to what extent, one is willing to share them.

2.3.5 DESIRE FOR PRIVACY

The desire for privacy is common to both animals and mankind. It has been suggested (McQuoid-Mason 1978 : 1) that in the animal world there exists a "biological right to privacy", which expresses itself in a desire for territoriality. Important aspects of this "animal privacy" are "personal distance", which is asserted between individual members of a group, and "social distance", which is observed between the different groups themselves.

Similar "distances" are found in human relationships.

The human animal has a dual nature. On the one hand, man is social and the acquisition of social competence is a measure of his attainment of humanity. On the other, every human individual is unique. What counts is that human beings are self-aware, and aware of their particularity. It is just as important for the individual to exercise and experience his uniqueness as it is for him to relate to the group. Socialization and individuation are the principle vectors in the development of the mature individual (Levine 1980 : 3).

The desire for privacy is natural and the inclination to pursue it follows automatically. This has always been the case, more so in modern times when life has become increasingly complicated and demanding. It has led further to a greater need for withdrawal and protection from the complications, demands and pressures of life. It is now recognized that the individual has not only a desire, but an absolute need for a shield of privacy behind which only he can retreat, and that this need should be translated into a right, regulated by the law or custom of the time (Young 1978 : 4).

Goffman (in McQuoid-Mason 1978 : 2) refers to an aspect of privacy in which he emphasises the "information preserve", as follows:

There is the content of the claimant's mind, control over which is threatened when queries are made that he sees as intrusive, noisy, untactful. There are the contents of pockets, purses, containers, letters and the like which the claimant can feel others have no right to ascertain. There are biological factors about the individual over the divulgence of which he expects to maintain control. And, most important ... there is what can be directly perceived about an individual, his body's sheath and his current behaviour, the issue here being his right not to be stared at or examined. Privacy is not merely an absence of information about an individual in the minds of others, but rather the individual's control over the information he has about himself.

In locating the problems of "privacy" at the level of "personal information", two questions arise: first, what is to be understood by "personal", and second, under what circumstances is a matter to be regarded as "personal".

2.4 PERSONAL INFORMATION

It is necessary for the purposes of the present discussion to outline the context in which personal information is used.

2.4.1 DEFINING THE TERM "PERSONAL"

The Oxford English Dictionary refers to "personal" as one of the meanings of "private" and vice versa. As Wacks (1989 : 22) notes, it is in three particular respects that its usage is of special importance here:

- It may mean that the matter is one which does not affect or concern the community. One might, for example, refuse to answer a question on the grounds that the subject is "personal".
- Certain activities may be characterized as private or personal (such as sexual or bodily functions) in order to claim the opportunity to withdraw physically to undertake them.
- Certain communications and conversations may be described as personal or private; a letter marked "personal" denotes that its contents are for the addressee's eyes only.

Describing a matter as "personal" in this way, is to bond it with characteristics of intimacy and sensitivity.

Wacks (1989 : 24) expands further on the definition of "personal":

There is a class of information that may be described as "personal". Normally it is objected that "privateness" is not an attribute of the information itself; that the same information may be regarded as very private in one context and not private in another. Naturally X may be more inclined to divulge his extra-marital affair or his homosexuality (or both!) to his psychiatrist or to his close friend than to his employer or his wife. And his objection to the disclosure of the information by a newspaper might be even stronger. The information remains "personal" in all three contexts. What changes is the extent to which he is prepared to permit the information to become known or to be used.

Any definition of "personal information" should refer both to the quality of the information and to the reasonable expectations of the individual concerning its use. The one is a function of the other. The concept of "personal information" functions both descriptively and normatively. Since "personal"

relates to social norms, to so describe something implies that it satisfies certain of the conditions specified in the norms. Thus if a letter is marked "personal" the implication is that it satisfies one or more of the conditions necessary for it being conceived as "personal".

2.4.2 DEFINING THE TERM "INFORMATION"

Much of the literature treats "information" as interchangeable with "data". It may be useful to distinguish between the two. "Data" become "information" only when it is communicated, received and understood. "Data" is therefore potential pieces of "information". Thus when the data assume the form of the printed word they are immediately transformed into information by the reader (Wacks 1989 : 25).

Collins English Dictionary (1992 : 251) defines information as:

Knowledge acquired through experience or study, knowledge of specific and timely events or situations; news, act of informing; condition of being informed.

The words "data" and "information" are used interchangeably throughout the course of this study.

2.4.3 DEFINING THE CONCEPT "PERSONAL INFORMATION"

Wacks (1989 : 26) provides the following definition of "personal information":

Those facts, communications, or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withhold or at least to restrict their collection, use or circulation.

According to Wacks (1989 : 27) an individual who regards information concerning his car as personal and therefore seeks to withhold details of the size of its engine, will find it difficult to convince one that his vehicle's log book constitutes a disclosure of "personal information".

This becomes even more difficult where the individual's claim relates to information which affects his private life. It would not be unreasonable, for an individual to wish to prevent the disclosure of facts concerning his trial and conviction for theft. Applying the proposed definition of "personal information" as a first order test of whether such information is "personal", may suggest that

the claim is a legitimate one. Such a claim is likely to be defeated on the grounds that in society, the administration of justice is an open and public process. The passage of time may alter the nature of such events and what was once a public matter may, several years later, be considered to be private. An individual may desire to withhold details of past offences by exercising his right to control "personal information" (Wacks 1989 : 27).

By voluntarily disclosing or acceding to the dissemination of personal information, the individual does not relinquish his claim to retain certain control over it. He may allow the information to be used for one purpose (such as medical diagnosis), but object when it is used for another (such as employment). Where he does not know that assessments have been made about him (for instance where he is described as a "bad risk" on the computerised files of a public authority), he may object to the use or disclosure of the information, particularly if it is misleading or inaccurate (Wacks 1989 : 27).

2.5 DEFINITION OF INFORMATION PRIVACY

A useful definition of information privacy which is endorsed in this study is that of Campbell et. al (1986 : 22) as:

The claim of individuals, groups, and institutions to determine for themselves when, how and what information about them is communicated to others.

2.5.1 THREAT TO INFORMATION PRIVACY

Young (1978 : 93) asserts that in recent years, it has become clear that the most powerful threat to individual privacy has come from the various departments of government. When one speaks with alarm about the "World of 1984" or of "Big Brother", one is really commenting on the ability of the State to encroach upon one's private life. The simple growth of population will make physical privacy harder to maintain, and as commercial transactions increase there will be greater opportunities for institutions (both public and private) to invade privacy.

Rowe (1972 : 22) shares this view when he remarks that the relationship between the State and the individual is unique and necessary; it is public institutions (government) rather than "private persons or institutions", which pose the most powerful threats to fundamental liberty.

The Fulton Report (in Young 1978 : 94) explains this position succinctly:

The role of government has greatly changed. Its traditional regulatory functions have multiplied in size and greatly broadened in scope. It has taken on vast new responsibilities. It is expected to achieve such general economic aims as full employment, a satisfactory rate of growth, stable prices and a healthy balance of payments... Through nationalisation it more directly controls a number of basic industries. It has responsibilities for the location of industry and for town and city planning. It engages in research and development both for civil and military purposes. It provides comprehensive social services and is now expected to promote the fullest possible development for individual human potential. All these changes have made for a massive growth in public expenditure. Public spending means public control. A century ago the tasks of government were mainly passive and regulatory. Now they amount to a much more active and positive engagement in our affairs.

In this modern era according to Young (1978 : 94) the State has responsibilities which encompass one's life from the cradle to grave. The Fulton Committee emphasised the point that public spending meant public control. This could be expanded to suggest that extended "public surveillance" is concomitant to public control; if the State is to accept these wide ranging responsibilities, there will be a

logical need for further information, research and documentation about social needs and demands.

The predominantly laissez-faire and regulatory policies pursued by governments in the eighteenth and nineteenth centuries required relatively less information about individuals, simply because governments felt little responsibility for individuals. As government activity increased so did the need for relevant information about the needs and circumstances of individuals (Young 1978 : 95).

According to Warner and Stone (1970 : 63) the growth of State activities has gone hand in hand with the increase of information collection. One could easily construct a long list of official record system for example, registers of births, marriages and deaths, passports, immigration records, criminal and court records, police files, television licences, gun licences, driving licences, medical records, school, college and university records, census data, tax records, and local authority records on rates, and building and planning applications.

Individually, they may record just a minor part of one's life, but collectively they represent a massive intrusion into private lives. And significantly, there is almost no control over the release of this information to the State,

since all of it can legitimately be demanded by the relevant government department. Submission of such information is an obligation of citizenship (Warner and Stone 1970 : 63).

2.5.2 STATE'S ROLE IN INFORMATION PRIVACY PROTECTION

According to the Report of the Privacy Protection Study Commission (1977 : 5) any government's expanding role as regulator and distributor of largess gives it new ways to intrude, creating new privacy protection problems. By opening more avenues for collecting information and establishing more decision-making forums at which it can employ such information, government has enormously broadened its opportunities both to help and embarrass, harass and injure the individual. These new avenues and needs for collecting information, particularly when coupled with modern information technology according to Sloan (1986 : 100) multiply the dangers of official abuse against which only legislation can protect.

Recent history demonstrates that these are real, not mystical dangers, and that while efforts may be made to protect citizens, the issue of information privacy must ultimately be sanctioned into law. If citizens still value their personal privacy, it is important that they take the initiative to make certain changes in the way

information about them is constructed, used and disclosed, particularly, since so much of an individual's life is now shaped by his relationship with public institutions (Report of the Privacy Protection Study Commission 1977 : 5).

The solution to this problem may be found in the adoption of a national policy for information privacy which is prevalent in western democracies (Sloan 1986 : 10). The features and objectives of a national policy is discussed below.

2.5.2.1 FEATURES OF A NATIONAL POLICY

If information privacy is to be protected, public policy must according to the Report of the Privacy Protection Study Commission (1977 : 13) focus on five systemic features:

First, while an organization constructs and keeps information about individuals to facilitate relationships with them, it also makes and keeps information about individuals for other purposes, such as documenting the organization's own actions and making it possible for other organizations, such as government institutions, to monitor the actions of individuals;

Second, there is an accelerating trend, mostly in financial areas, towards the accumulation of information that includes more personal details about an individual;

Third, more and more information about an individual is collected, maintained, and disclosed by organizations with which the individual has no direct relationship, but whose records help to shape his life;

Fourth, most information gathering organizations consult the records of other organizations to verify the information they obtain from an individual, and thus pay more attention to what other organizations report about him than to what he reports about himself; and

Fifth, neither law nor technology now gives an individual the tools he needs to protect his legitimate interests in the records organizations keep about him.

2.5.2.2 OBJECTIVES OF A NATIONAL POLICY

According to Sloan (1986 : 17) every member of a modern society acts out the major events and transitions of his life, with organizations as attentive partners. Each of his countless transactions with them leaves its mark in the records they maintain. Never before have so many organizations had the facilities for keeping available

the information that makes it possible to complete on a daily basis, a multitude of transactions with a multitude of individuals, and to have the relevant facts on each individual available to inform subsequent decision-making about him.

If the information-gathering organization is part of the public sector, the individual may have no alternative but to yield whatever information is demanded of him. He has even less practical control over what actually gets into the records about him, and almost none over how the records are subsequently used. He can seldom check on the accuracy of the information, or discover and correct errors and misconceptions, or even find out how the information is used, much less participate in deciding to whom it may be disclosed (Report of the Privacy Protection Study Commission 1977 : 14).

According to the Report of the Privacy Protection Study Commission (1971 : 15) an effective privacy protection policy must have three concurrent objectives:

- to create a proper balance between what an individual is expected to divulge and what he seeks in return (to minimise intrusiveness);

- to open up record keeping operations in ways that will minimise the extent to which recorded information about an individual is itself a source of unfairness in any decision about him made on the basis of such information (to maximise fairness); and
- to create and define obligations with respect to the uses and disclosures of recorded information about an individual (to create legitimate enforceable expectations of confidentiality).

If South Africa wishes to embark on a full scale investigation into the adoption of a national policy on information privacy, it would be wise to take cognisance of these fundamental characteristics.

2.6 SUMMARY

Privacy is a universal phenomenon. There are three types of privacy viz. territorial privacy, privacy of the person and information privacy. This chapter focuses on information privacy, which involves the rights of individuals in relation to information about them that is circulating throughout society.

Absolute privacy is impossible: civilised behaviour requires at least some exchange of ideas and information

between citizen and government.

Today, the government has responsibilities which encompass one's life from cradle to grave as it regulates and supports large areas of economic and social life. Because many of the services offered by public institutions are considered necessities, the citizen has no choice but to submit to whatever demands made of him. One such demand is the need to divulge personal information in exchange for the services rendered by the public institution. This leads to an increase in the extent of government involvement in private affairs, but this might be thought to be a reasonable price to pay for the ensuing economic and social benefits.

Undoubtedly the possession of information implies the possession of power. Government has enormously broadened its opportunities both to help and embarrass, harass and injure the individual. These opportunities include inter alia., when they become privy to the personal details of a citizen's life, when personal information furnished by the citizen for one purpose is used for another, and when personal information is shared with other government departments without their knowledge or consent. The government has the opportunity to violate the personal privacy of the citizen, of which he knows nothing.

It is important that adequate safeguards are introduced to address the privacy problem. A national policy on information privacy protection is a vital safeguard to prevent the abuse of personal information.

The best safeguard is not that the government know less about the citizen, but that the citizen know more about them, and that he is aware of what they know and how they use such information.

It is important when considering privacy in the context of the relationship between individuals and governments, to debate not "which affairs should be subjected to government scrutiny", but "what safeguards should apply in the collection, storage and application of such information"?

CHAPTER 3

TECHNOLOGICAL CHANGE - COMPUTER REVOLUTION

After the enemies with guns have been wiped out, there will still be enemies without guns; they are bound to struggle desperately against us and we must never regard them lightly.

Mao Tse Tung (in Young 1978 : 309)

Men feed data to a computer and men interpret the answer the computer spews forth. In this computerized age, the law must require that men in the use of computerized data regard those with whom they are dealing as more important than a perforation on a card.

A judgement of the Supreme Court -
Kentucky (in Young 1978 : 319)

3.1 INTRODUCTION

The revolution in information technology is no accident in a society so vast in population, so complex in organization, so vulnerable to the slightest breakdown in the co-ordination of individuals and institutions and the delivery of services and the maintenance of security. Such

a society has a voracious and expanding need for information. It is natural that it would support the development of a vast arsenal of material which gathers, stores, classifies, analyzes, retrieves, and puts out information. If one compares society with a machine, information is the oil, grease, and fuel on which it runs; if the comparison is with an organism, information is its life's blood (Martin 1988 : 53).

According to Bier (1980 : 13) the folk-wisdom that a secret, once told, is no longer a secret, has never been more true than in modern society for the essence of secrecy is control over who knows the secret. Today, no one knows any longer who has access to what information and for what purposes. Although the data-gathering of government begins with a rational need to know, the unknown ramifications of data bank exploitation are a real threat to the individual.

An attempt is made in this chapter to examine the impact of technological developments and the consequences that arise from the use of computers to store large quantities of information about individuals or organizations, and to assess the possible dangers of such use and abuse.

3.2 DEFINING TECHNOLOGY

Technology is the practical application of scientific research. It may take the form of either inventions (new devices) or innovations (new methodology). While technology tends to be for the most part associated with physical device, it is important to realize that it can be intangible in nature (ie. procedures or techniques). Every physical device creates a set of procedures or techniques that become an integral part of that technology. Such procedures become enshrined as traditions, roles, and skills (Naidoo 1987 : 39).

Webster (in Naidoo 1987 : 39) defines technology as follows:

The systematic treatment of an art; applied science; a technical method of achieving a practical purpose; the totality of the means employed to provide objects necessary for human sustenance and comfort.

From the above definition it can be deduced that technology is broad, covering the systematization of experience as well as those developments which require research to further scientific knowledge, in order to deal with particular problems.

3.2.1 REASONS FOR THE USE OF TECHNOLOGY

Technology increases productivity. It allows more work to be accomplished for a smaller investment of resources, in less time, or with better quality result. Technology serves to extend human capabilities. Automobiles extend the ability to walk, telephones extend the ability to talk and listen over a distance, and nuclear technology extends the ability to harness energy. At the core of all technologies are human capabilities: technology cannot function otherwise. This point is fundamental to the successful use of technology (Naidoo 1987 : 44).

3.2.2 IMPACT OF TECHNOLOGICAL DEVELOPMENTS ON THE RIGHT TO PRIVACY

Sloan (1986 : 1) asserts that an aspect of Orwell's 1984 was its implication that "Big Brother" is a stage in the evolving role of government. As technology advances, the problem shifts from the exertion of governmental authority over property rights to the potential for governmental intrusion on individual privacy rights.

According to Justice Douglas (in Sloan 1986 : 1):

The central problem of the age is the scientific revolution and all the wonders and the damage it brings. The machine which Orwell once called the genie that man has thoughtlessly let out of its bottle and cannot put back again, has perpetuated new concentrations of power, particularly in government, which utterly dwarf the individual and threaten individuality as never before. Where in this tightly knit regime, is man to find liberty?

On the subject of privacy and its place in the society of the future, Justice Douglas (in Sloan 1986 : 3) observes appropriately:

We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government. The aggressive breaches of privacy by the government increase by geometric proportions.

Sloan (1986 : 3) states that the technological capability to collect, maintain and disclose vast quantities of information about private lives has far out-paced the legal protection of privacy. Many information systems containing sensitive data are being constructed to facilitate important social objectives, such as better law enforcement, faster delivery of public services, more

efficient management of credit and insurance programmes, improvement of telecommunications and streamlining of financial activities. These high technology systems are also being used at an increasing rate by public authorities to enhance their control of the lives of individuals. The growth of data banks and vast computerised pools of information about people in every aspect of their lives is probably the single most important element in the contemporary range of concerns about the right of privacy.

3.2.3 PROBLEMS OF PRIVACY IN A TECHNOLOGICAL AGE

According to Bier (1980 : 194) not so very long ago, a person who wanted to keep some information from being generally available knew how to do so. The drawn shade and the closed door preserved the privacy of his behaviour; the locked drawer contained his confidential documents; and only the ear of a trusted ally heard his secrets.

Government always had resources outstripping those of a single individual, essentially it was a matter of the eye, ear, and brain of one human being matched against the eyes, ears, and brains of other human beings. In that sense, the competition was reasonably equal.

In his unceasing quest for knowledge, man has created a crude model of his own brain, and found, to his wonderment, that it can compute with an accuracy and speed which he can

barely imagine, and can remember with an exactitude which embarrasses human recall (Bier 1980 : 194).

While rejoicing in the benefits brought about by these new and powerful tools, mankind has become uneasy. Human capabilities could be controlled, but a lack of familiarity with the capabilities of the new information technology, means that its control lies exclusively in the hands of those who have specialized access to it. The individual who wishes to keep personal data to himself is no longer dealing on equal terms with his own kind: he is matched against machines (Bier 1980 : 194)

3.3 COMPUTER TECHNOLOGY

The term "computer" needs to be highlighted before an attempt is made to discuss computer technology.

3.3.1 PURPOSES OF COMPUTERS

Naidoo (1987 : 45) defines the computer as:

Any calculating device. The term is derived from the Latin word computaire, meaning to reckon or compute, and can as appropriately be applied to an abacus or an adding machine. However, the term "computer" has come to mean a special type of calculating device, having

certain definite characteristics.

Flaherty (1979 : 122) asserts that the computer is a machine which solves problems through its interaction with man by a series of instructions in the form of a programme.

It can be deduced that the computer has the following distinct characteristics:

- (a) speed of operation;
- (b) ability to store and retrieve information;
- (c) ability to handle large and complicated information;
- (d) facility for calculation; and
- (e) accuracy.

3.3.2 DEFINITION OF COMPUTER TECHNOLOGY

According to Naidoo (1987 : 47) computer technology encompasses a complex, interdependence system composed of people (e.g. users, computer specialists, managers); equipment (e.g. hardware such as computer mainframes and peripherals); software, such as operating systems, application programmes and data), and techniques (e.g. procedures, practices and organizational arrangements).

A more inclusive definition of computer technology would include organization and networks that comprise the broader "systems world" of computing, and that constitute the

societal infrastructure for application of the technology within specific organizations (Naidoo 1987 : 48).

3.3.3 ADVENT OF THE COMPUTER AGE

Young (1978 : 95) asserts that the government's appetite for information about citizens and its capacity to digest this data, has increased. The advent of the "computer age" is especially significant. The tremendous capacities and potential implications of computers for privacy is significant.

Arthur Miller (1971 : 38) sees the development of government computer systems as being the single greatest threat to man's privacy:

As the capacity for information handling increases there is a tendency to engage in more extensive manipulation and analysis of recorded data which, in turn, motivates the collection of data pertaining to a longer number of variables.

The utilization of computers in government record systems has over the years become widespread. From the standpoint of the public administrator there are significant benefits to be gained from the employment of such devices. There is nothing sinister about a computer itself, since it is

simply a sophisticated machine for storing and collating huge volumes of information. There are benefits to administrators and society alike in being able to run immediate checks and cross checks on such records as criminal, police or social security files, especially where there is increasing population mobility (Young 1978 : 95).

Rowe (1972 : 13) is of the opinion that citizens expect the State to provide them with a whole range of services. This range broadens annually, and the price to be paid for this is the increasing restrictions upon civil liberties, including privacy. The computer is no more and no less than a tool of man's devising. Some people believe it is the most wonderful of all tools, able to confer benefits on mankind which are even beyond their conception. Others concede the benefits, but are more troubled by the potential threats.

According to Sieghart (1976 : 3) like all tools, the computer itself is morally neutral. How it will affect society depends on what people want to do with it, what they are able to do with it and ultimately what society allows them to do with it.

The computer in the present day world is a very recent development. It has had an immediate influence upon privacy issues. Madgwick and Smythe (1974 : 20) claims

that:

Of all the threats posed to privacy in a rapidly changing and developing world, none is more sinister in its potential, more far reaching in its implication, than the computer.

3.3.3.1 COMPUTER AND ITS CONTEMPORARY IMPACT ON PUBLIC ADMINISTRATION

According to Warner and Stone (1970 : 63) all the events and transactions in a person's life, have become part of some official file. Considering how this happens is relevant to the present study.

To start with, the duly recorded certificate of birth of a child immediately gives rise to hospital and other medical records of ailments, treatments and immunizations. One represents an extra allowance against his parent's income tax, and is monitored to see where the family might settle when school going age is reached. Once there, he generates record after record concerning his attendance, I.Q. Tests and his prowess from "could do better" to "couldn't be worse", much of which he hopes would be forgotten in later life (Warner and Stone 1970 : 63).

As soon as he is old enough, he gets himself jobs for weekends and the holidays, opening up a new record trail that will be followed for years, of social security, tax and employment. Approaching adulthood, he saves up for his first old car, which he has to insure, and be licensed to drive. He becomes a registered elector; he will apply for a marriage licence; he may later collect divorce decree, which creates voluminous documentation. From house to house, and from job to job, he moves; and some trace of this is left in the archives of the nation (Warner and Stone 1970 : 64).

The adult may avoid a criminal record - though even such a minor offence as a parking fine may serve to place him, irrevocably, on the police files. He would be very lucky to avoid adding to his medical records (Warner and Stone 1970 : 65).

Madgwick and Smythe (1974 : 28) state that it is possible to draw up an impressively detailed personal profile of an individual, from files that are available for public inspection. Access to a file cabinet is achieved by walking to it. Access to computer files is achieved by sending a request to the machine. This is a risk, and a danger to privacy.

The citizen's understanding, when he supplies information, is that such information is intended for a particular purpose and will not be exhibited beyond that immediate intent without his consent. The possibility of it escaping to any other party is not something which he should have to envisage. Any such unauthorised use is misuse: it is a breach of privacy one is entitled to expect, and an infringement of such remaining freedom as he has to reveal what he chooses to whom he chooses (Madgwick and Smythe 1974 : 29).

3.3.3.2 COMPUTERS AND THE STORAGE OF INFORMATION

According to Sloan (1986 : 23) society's concern is with those computers which are used in offices to replace conventional filing systems. The computer must be able to compare favourably with all the best features of the best document-filing system. It must also perform them faster, and require fewer staff to maintain it.

Organizations are forced, by the constant search for efficiency, to make use of the best available tools. There was no relief from the weight and acreage of paper. As computers developed, they reduced that burden. With virtually no limit either on the amount of information they can hold, or on the distance over which they can collect and despatch it, thousands of pieces of paper can now be

abandoned (Warner and Stone 1970 : 52).

The increase in the flow of information induced by the computer threatens the individual's ability to control the flow of information about himself. In other words, his privacy is endangered. If computers were used to store no more than scientific or numerical information, or information already in the public domain, they would represent no problem affecting privacy. It is storage of "the facts of his personal life" that give rise to the privacy fears (Rowe 1972 : 19).

Rowe (1972 : 20) aptly states that individuals are anxious to enjoy the benefits that an increased information flow can confer:

As populations and mobility increase, there will be other incentives to establish central data files, for these will make it easier for the consumer in new environments to establish who he is and thereby to acquire quickly those conveniences which follow from a reliable credit rating and an acceptable social character. At the same time, such central data files will make it easier for governmental officials to ensure his security, since he will know at all times with whom he is dealing. In consequence we can expect a great deal of information about the social, personal,

and economic characteristics of individuals to be supplied voluntarily - often eagerly - in order that, wherever they are, they may have access to the benefits of the economy and the government.

3.3.3.3 COMPUTERS AND "PROVISIONAL CATASTROPHE"

Pitt and Smith (1984 : 28) are of the view that the computer's power brings a new threat. It offers much in the way of increased freedom and improved social amenities, yet ironically, if it is misused, it could deprive one of freedom.

The possession of information is the possession of power. No country can be run, no business managed, unless there is a constant supply of information to assist the processes of decisionmaking. Authority and control cannot be maintained, nor alternative future policies evaluated, in the absence of an information flow. In recent years that flow has increased to a torrent in all channels of administration (Warner and Stone 1970 : 15).

A significant reality is that a computer has no mind of its own, no will of its own, no philosophy of its own; it has "no artificial life". It cannot be "taught", nor can it "think", in any profound human sense. People are in control, all the time (Warner and Stone 1970 : 17).

The threat to the individual comes primarily from the State, from the increased power put into its hands by the use of computers. Both government and business or private administration could have instantly available all the recorded facts about everyone, literally from the cradle to the grave (Pitt and Smith 1984 : 28).

Warner and Stone (1970 : 20) asserts that the State could maintain an integrated dossier file on every member of the population using computer equipment. Consequently, a massive integrated computer "data bank" could come into being. Here, then is the "catastrophic" threat to freedom and privacy. This integrated computer data bank "put one's whole life history no further than the push of a button away".

The biggest fact-gathering organism of any kind is the government. It is in that institution, at all levels, that one can see the computer is most welcome for its power to cope with personal files and to relieve clerks of the oppressive burden of paperwork (Sloan 1986 : 28).

3.3.3.4. EFFECT OF INFORMATION IN COMPUTERS AND ITS IMPLICATION FOR PRIVACY

Sloan (1986 : 7) asserts that personal information in a file may be neither accurate nor current, but since it is not regularly reviewed, the recipient of information about a particular person tends to regard it as unchangeable.

A similar difficulty derives from the incomplete nature of some of the information, particularly in the area of arrest records. A dossier might well contain the information that a given individual was arrested on criminal charges and sentenced to three months in prison. This might be factually correct. What is not revealed, however, is the equally important explanation that the arrest took place during an anti-war demonstration or desegregation rally and that the charges were later thrown out, or that the statute that permitted the arrest was overturned. Readers of the record are not always equipped or even motivated to verify the accuracy of what they read. The simple fact that information appears in somebody's file constitutes an evaluation in itself (Sloan 1986 : 7).

Information files about individuals according to Sloan (1986 : 10) have been found in industrial societies for a long time. Long before computers revolutionized the technology of record keeping, government, businesses, social service organizations, schools and the like maintained historical records about people that were usually detailed and comprehensive.

A great number of people are deeply concerned about the abuse potential of dossiers and data banks in all areas of life, the scope of collecting and distributing information still appears to be largely discretionary. Until such time that there are substantive legal safeguards to control the use of stored data, the dangers of serious violations of personal privacy will continue to be a problem in this technological age (Rowe 1972 : 30).

It seems far from clear how privacy can have anything new to fear from the advent of the electronic computer. If computers have anything to do with privacy, then it must be with an aspect of privacy which is not directly derived from any notion of physical intrusion or surveillance (Sieghart 1976 : 15).

The grounds on which the debate about privacy and computers is fought, is on the privacy of information, based on the classical definition propounded by Westin (1970 : 7):

The claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.

Campbell et. al (1986 : 36) state that most people know computers store personal medical information, tax and financial details, social security and employment records,

police criminal records and other intelligence records. But very few outside the departments are aware that several large government computer complexes are being expanded and interconnected, which will result in the linkage of important distinct record systems.

According to Hamelink (1984 : 19) linkages between different computer data banks already exist. By the year 2000, public sector data banks will probably store more than 600 gigabytes (about one hundred thousand million words) of personal information, accessible from a hundred thousand computer terminals; and no one will be excluded. Central government will remain the largest holder and processor of personal information for the foreseeable future, followed closely by other public institutions such as the police department and intelligence services.

For the individual according to Hamelink (1984 : 20), there is a balance of advantage and risk. Much information is held for the benefit of the person named on a computer record (data subject), for example to provide appropriate health care or to grant correct welfare benefits. But many data banks are concerned almost entirely with information of which the holding is at worst to the disadvantage of the individual concerned. The most sensitive personal data often held by institutions are the least regulated.

According to John Shattuck of the American Civil Liberties Union (Campbell et. al 1986 : 37):

Power may come out of the barrel of a gun, but far more power comes out of computer or databank, particularly if the information in it relates to people who do not know that it has been collected or cannot challenge its accuracy or use.

3.3.3.5 COMPUTER LINKAGE OR COMPUTER MATCHING

Hamelink (1984 : 87) states in recent years a technique known as computer matching or computer linkage is emerging. This involves:

The electronic comparison to two or more sets of separate and unrelated records. This technique make it possible to screen, almost instantly, vast and disparate sets of personal information in search of similarities and differences.

Through computer matching it is possible to build up a picture of an individual citizen's life-style, habits and relationships of which he knows nothing but which is used in making decisions about his military service or welfare grant (Hamelink 1984 : 87).

Hamelink (1984 : 88) is of the opinion that computer matching makes it possible for the linker to consider a lifetime of information when making a decision about a citizen. This information may include dated records of minor traffic offences and health problems, all of which may unfairly reflect on the current situation of the individual concerned. The connection established between various items of information concerning a citizen is used as a basis for passing judgement on him, a secret judgement against which there can be no appeal and which, because it is provided by a computer is thought to be objective and infallible.

The Privacy Commissioner of Canada (in Bayat and Sing 1994 : 360) advocated that computer matching be challenged as a tool even to achieve desirable goals. The reason is that it violates the individual's right to prevent information being used without his or her consent for purposes other than for what it was collected.

3.4 TRANSBORDER DATA FLOWS

Wacks (1989 : 204) states that a growing international trade in information and data processing services ensures that data are no longer confined within national borders.

Information is transferred from the originating computer in country A to the "host" computer in country B where they are stored or processed and then either returned to the originating computer or redistributed to a computer in country C (and /or D, E). Whilst most data transferred tends to be of a technical nature, personal data may also be moved to a so-called "data haven", a country which has little or no control over data banks, thereby evading regulation in the originating country. The only effective means of controlling transborder data flow is through international convention (Hamelink 1984 : 94).

3.4.1 REMEDIES

Attention will now be focused on steps that have been introduced to address the problems associated with transborder data flows.

3.4.1.1 INTERNATIONAL INSTRUMENTS

Two principal international instruments will be discussed in this section, namely, the Guidelines on the Protection of Privacy and Transborder Flows of Personal Information (hereafter called the Guidelines) adopted by the Council of the OECD on 23 September 1981, and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereafter called the

Convention).*

The Guidelines according to Wacks (1989 : 207) seek to attain four main objectives: to protect the "privacy" of personal data; to foster the free flow of information; to avoid unjustified restrictions on this free flow caused by domestic "privacy legislation", and to harmonize the provisions of various domestic laws. They are intended to form the "minimum standards" of legislation in OECD countries and have been followed by a Declaration on Transborder Data Flows which was adopted by OECD Member States on 11 April 1985. The latter commits them to the introduction of general regulation of the transborder movement of data.

The Convention according to Wacks (1989 : 208) seeks to:

Secure in the territory of each party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

* **A detailed analysis on the Protection of Transnational Data Flows is provided in the appendices of this study.**

A summary of the relevant principles contained in these documents are referred to below.

3.4.1.2 TRANSNATIONAL DATA PROTECTION PRINCIPLES

The general principles to be found in the domestic legislation of most industrialized states match those expressed in the Council of Europe Convention and the OECD. These principles according to Wacks (1989 : 208 - 209) include:

- Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject;

- Data quality principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date;

- Purpose specification principle

The purpose for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose;

- Use limitation principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Guidelines except where:

- (a) with the consent of the data subject;
- (b) by the authority of law;

- Security safeguards principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data;

- Openness Principle

There should be a general policy of openness about development, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purpose of their use, as well as the identity and usual residence of the data controller;

- Individual participation principle

An individual should have the right:

- (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- (b) to have communicated to him, data relating to him
 - (i) within a reasonable time;
 - (ii) at a charge, if any, that is not excessive;
 - (iii) in a reasonable manner; and
 - (iv) in a form that is readily intelligible to him;
- (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial;

(d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended;

- Accountability principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

3.5 EXAMPLES ILLUSTRATING THE INAPPROPRIATE, UNAUTHORISED OR ILLEGAL ACCESS TO AND USE OF PERSONAL INFORMATION

From the examples analyzed below, it comes to light that information privacy demands serious attention (Bayat and Sing 1994 : 360):

- a nursing home resident in the United States of America lost government medical assistance after her bank and welfare records were matched. What the match did not reveal was that some of the money in her savings account was exempt from asset calculations because it was held in trust for burial expenses;
- a man was arrested for being absent without leave from the marine corps of the United States 11 years after he had been legally discharged. A computer matching

programme found him to be absent without leave. He was held for five months before the error was corrected;

- two complaints were made to the Privacy Commissioner of the Wanganui Computer Centre concerning the incorrect description of offences for which convictions had been entered. These resulted from the coding system for related or similar offences. The original text in each case was corrected to show the true nature of the offence, for example, possession of cannabis for own use instead of possession of cannabis for purpose of supply, and common assault instead of aggravated assault;

- a trainee terminal operator at the Wanganui Computer Centre admitted to making queries on the computer about his friends and relatives, and verbally passing some of this information to other members of the family in the course of general conversation;

- early in 1986, 15 000 Swedes discovered that they had been unwitting guinea pigs in a sociological survey. The project continued under three successive governments over a period of 20 years. The personal numbers of most Swedes are recorded in over 100 data banks in the public and private sectors. Medical, educational, welfare, police, employment and other records were accessed without consent in this secret survey; and

- a New Orleans sculptor was afraid to travel to Mexico to meet his fiancée's grandparents. When crossing the border some years ago, he had been seized at gunpoint by the police and jailed. The problem was that a federal computer identified the sculptor as a fugitive because a real fugitive sometimes uses his name and social security number.

3.6 INFORMATION PRIVACY PROTECTION PRINCIPLES

Studies on the abuse of information technology and private interests have indicated that the assurances sought by the individual citizen can be provided by the successful application of certain principles.* Sieghart's (1976 : 11) formulation of these principles is as follows:

- Principle of public notice: All computer systems holding personal information should be publicly known;
- Principle of correct data: Personal information held in computer systems should be accurate, complete and up to date;

* **A detailed analysis of Information Privacy Protection Principles are found in the appendices of this study.**

- Principle of security: Personal information held in computer systems should be adequately secured against unauthorized access;
- Principle of legitimacy: Personal information in computer systems should be collected and used only for legitimate purposes;
- Principle of minimum data traffic: Personal information should pass through computer systems only to the minimum extent and for the minimum time necessary for legitimate purposes;
- Principle of subject verification: The data subject should be able to verify and correct all information held about him in any computer system, and discover how it has been used; and
- Principle of independent supervision: Someone independent should be able to enforce these principles fairly.

3.7 SAFEGUARDS

According to Rowe (1972 : 22) there are a number of ways in which the individual's privacy can be protected. These lie in establishing good professional standards, building

in technical safeguards and adopting secure administrative procedures.

Attempts are being made to establish a professional code for computer programmers. The need for rigorous professional training and a code of professional ethics is widely recognized (Sloan 1986 : 49).

According to Rowe (1972 : 22) technological safeguards are the next most important means of safeguarding the security of sensitive data. By this is meant that hardware and software techniques which limit access to authorized and identified persons, control the processes which are carried out on the files, and monitor the performance of the system so as to detect unusual, suspicious or unauthorized activity. None of these technological safeguards guarantees that unauthorized access will be prevented; they serve to ensure that the task of penetrating the system is sufficiently difficult and time consuming, and carries a risk of detection, that it is not worth undertaking.

Laver (in the International Social Science Journal 1972 : 430) has compiled a list of administrative safeguards which could be introduced as a set of model rules for operating computers containing personal information. He proposes that an independent advisory council should have to be satisfied of the need for the

data and of the effectiveness of the security measures before authorization would be given to hold personal data in computers. He also proposed coded identifications rather than names and addresses and that personal files should be erased at regular intervals of not more than ten years.

Martin (1984 : 67) asserts that legal remedies and sanctions is an essential safeguard in minimising the dangers of databanks.

Another principal mechanism discussed by Sieghart (1976 : 126) as an attempt to resolve this issue is the appointment of an ombudsman who may ask for legal sanctions to ensure that:

- public authorities announce what classes of information they collect for what administrative or other purposes;
- public authorities need to tell the citizen what information they hold about him;
- when collecting information, these authorities tell the respondents what are their legal obligations to provide the information, and whether they can refuse to give them;

- information no longer needed for the purpose for which they were collected are erased or rendered inaccessible;

The vital protection that an individual requires is the right to know that information is stored about him, and the right to verify that information. This view is expressed by Westin (1970 : 144) as follows:

When the information keeper knows that the individual will be notified, can see and can challenge the information, all the restraints of visibility of action will be on the keeper. His loss of anonymity will be the best guarantee of fairness and care in the information keeping procedure.

According to Rowe (1972 : 22) the problem of computers and privacy is one of knowing where to strike a balance between the interest of the individual in keeping his affairs to himself and his interest in revealing his affairs to others so that he may enjoy the fruits of the more efficient and more informed society that results.

Rowe (1972 : 22) states that it is not clear at present where the most satisfactory balance will be found. What is clear is that without some safeguards and restraints, the benefits that the computer can bring to society will be accompanied by a loss of individual privacy that many

find unacceptable.

3.8 SUMMARY

Technology is the practical application of scientific research. It increases productivity in that it allows more work to be accomplished for a smaller investment of resources, in less time, or with better quality results.

Citizens expect the State to provide them with a whole range of services. As a result government's need for information about citizens and its capacity to digest this data, has increased. Public institutions are forced, by the constant search for efficiency, to make use of the best available tools. One such tool is the computer.

The computer is morally neutral, how it will affect society depends on what people want to do with it, what they are able to do with it and ultimately what society allows them to do with it.

The threat to the individual comes primarily from the State, from the increased power put into its hands by the use of computers. The State maintains an integrated dossier file on member of the population by using computer equipment. In this way the computer has given bureaucracy the potential for omniscience, if not omnipotence, by

dropping into its hands the power to know.

Data collected for different purposes may be collated to build up a picture of an individual's life style, habits and relationships of which he knows nothing but which is used in making decisions about him. There is at present little or no protection for citizens against information they have supplied in all innocence or that has been collected without their knowledge being used for purposes hostile to their interests. A further danger in this regard is when the information used to pass judgement on the citizen is incorrect, inaccurate or irrelevant.

The threat posed by the possibilities for misuse of information technology to liberty and privacy relates to three of its features: the huge storage capacity of computers together with their ability instantly to collate and produce any part of what is stored; the ease with which systems can communicate with one another; and the extensive means available for the rapid dissemination and presentation of information.

Most people know that computers store medical, educational, and tax records. What they don't know is that data banks are created, whereby information can be exchanged and interconnected with data banks of international countries. Transnational data protection principles are necessary

mechanisms to protect the processing of personal information across borders.

Studies on the abuse of personal privacy indicate that the assurances sought by the individual can be provided by the application of information privacy protection principles.

Other safeguards to protect the personal privacy of citizens include the creation of professional training and ethics for computer programmers, an independent advisory authority to protect personal information, computer codes so that the identity of the person concerned is protected and legal remedies to minimise the dangers of data banks. The further appointment of an ombudsman will serve to protect and preserve the personal privacy of citizens.

It is ultimately the attitude of administrators, not the nature of computer systems, which creates the threat to privacy.

CHAPTER 4

FREEDOM OF INFORMATION

The government did not tell
because it was not asked;
it was not asked
because what was going
on was not known.

Anon

4.1 INTRODUCTION

Freedom of information is a fundamental human right and is the touchstone of all freedoms to which the United Nations is consecrated (Horn and Gruber 1990 : 9).

According to Sieghart (1988 : 95) this concern is reflected in Article 19 of the Universal Declaration which guarantees the right to "seek, receive and impart information". The UN International Covenant on Civil and Political Rights provides that:

Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print,

in the form of art, or through any other media of his choice.

McCamus (1981 : 6) is of the opinion that access to public information is defended so that people may individually or collectively exercise other "rights": to make governments accountable, to be able to defend themselves when the public authorities subject them to deprivations, to organise themselves to displace incumbents of public office, or to discover how they can take advantage of public benefits under law available to them.

Lippmann (in McCamus 1981 : 6) remarks that:

The government must be able to govern and the citizens must be represented in order that they shall not be oppressed. The health of the system depends upon the relationship between those two powers. If either absorbs or destroys the function of the other, the constitution is deranged.

McCamus (1981 : 1) is of the view that the citizen has two rights. One is to be governed effectively and the other is to be so governed that he is not "oppressed".

In this chapter attention is focused on providing a definition of freedom of information. A detailed analysis

is also provided on freedom of information and accountability, and freedom of information and public administration.

A definition of freedom of information is now proposed.

4.2 DEFINITION OF FREEDOM OF INFORMATION

The term is, in many ways, all-embracing, and has come to mean many things to many people.

Riley (1986 : 1) defines freedom of information as follows:

To those in the media, and to others, it implies the right to publish information and the free flow of information without undue government restrictions. It means the right to inform the public without being fettered by regulations which in any way restricts this right. In another context, it has come to mean the free flow of information across borders unfettered by government regulations.

4.3 FREEDOM OF INFORMATION

Riley (1986 : 2) is of the view that access to information is a right asserted upon the requirement of accountability which will be meaningless unless there exists a legal right

of access to government information. The argument is that without such a right a government will be able to manipulate information for its own ends, mainly to preserve itself in office. This danger is considered to be so great as to require legal access to government information, even if this involves certain costs. The ability of governments to manipulate information is seen as opposed to the rule of law: it is arbitrary. Arbitrariness is associated with despotism and not democracy.

Delbridge and Smith (1982 : 28) states that without legal access to government information, it is feared that governments will use information selectively, releasing only that information which is to their credit or undermines the credibility of their opponents, and that this reduces the requirement of accountability.

The objective of a public right to know is the prevention of the manipulation of information, or arbitrariness, and to give substance to the democratic requirement of accountability. Democracy requires the creation of a legal right of access to government information (Robertson 1982 : 11).

4.3.1 DISCLOSURE OF GOVERNMENT INFORMATION

Harrison (1988 : 39) asserts that a high degree of

disclosure of government information is justified because it is seen as expressing and fulfilling certain values. These values according to Jones (1989 : 39) are associated with other values such as participation, knowledge and freedom of ideas.

It is argued that government secrecy produces apathy and ignorance. It is further argued that these are dangerous to democracy since they produce a citizenry who will be unwilling and unable to participate in political life, participation being seen as a fundamental requirement of a democratic polity (Harrison 1988 : 39).

Absence of participation will produce a separation of government from the people leading to a "credibility gap" and a breakdown of communication between government and people (Delbridge and Smith 1982 : 30).

According to Robertson (1982 : 12) governments will cease to be responsive to the electorate, and will treat the people with disdain because they see the people as ignorant and uninterested. This is seen as the end of popular government, an essential requirement of democracy. It is also seen as a situation in which the citizen does not develop, become more mature, responsible or aware, and that democracy ought to be a political system in which individuals learn and become "better citizens". This they

will fail to do without participation.

Disclosure is valued because of the kind of person and citizenry which it will create - one which is active, lively and knowledgeable and to give substance to the democratic requirement of participation. Its implication is that a good society requires the maximisation of the free movement of ideas and knowledge (Harrison 1988 : 41).

4.3.2 DISCLOSURE OF GOVERNMENT INFORMATION AS A MEANS

Robertson (1982 : 12) states that democracy requires the disclosure of government information because it is a means of ensuring that the actions of government will be representative of the interests of the citizenry. It is a means of checking on the "rationality" of government actions, that government actions are being taken on the best available information. Government secrecy then raises the question of what the government has to hide.

Disclosure as a means help to prevent governments from abusing office or acting against the interests of individual citizens. It is also a means of giving substance to the democratic requirement of representation. The implication is that government secrecy is evidence of the fact that the government is doing something which it could not justify to the public (Harrison 1988 : 42).

4.3.3 CRITICISMS OF DISCLOSURE OF GOVERNMENT INFORMATION AS A RIGHT

According to Robertson (1982 : 13) the problem with the argument that the citizen has a right to know is that it fails to solve the problem of what is the appropriate balance between secrecy and openness.

The problem is that one cannot eliminate all discretion since politicians will keep certain aspects of their thinking secret and discussing certain of their plans with others of a like mind, in secret. **There can never be, a right to know all that a citizen might like to know. There can only be a right to know certain specified and carefully defined types of information** (Robertson 1982 : 13).

4.3.4 FREEDOM OF INFORMATION AND ACCOUNTABILITY

The freedom of information debate according to McCamus (1981 : 1) has raised searching questions concerning the accountability of a modern government to its electorate. Some participants in the debate argue that the traditional mechanisms of accountability - elections, opposition parties, and a free press are no longer adequate.

The complexity of the social and economic problems governments are asked to solve often place severe strains on the critical assessment of the conduct of public affairs. Greater access to government information would provide additional opportunities for democratic supervision of governmental processes and activity (McCamus 1981 : 1).

On the other hand, others have argued that the traditional mechanisms of accountability and control do provide adequate safeguards, given the need to balance the democratic concern with accountability against the public interest in ensuring that government has the ability to carry out its mandate effectively (McCamus 1981 : 2).

According to Riley and Relyea (1983 : 10) there are two requirements of accountability, each with a direct and immediate implication for freedom of information policy:

First, there would be clear and well understood relations within the government and the citizenry so that specific groups of governmental actors could be held responsible for particular categories of actions taken by the public authorities. This is the structural requirement of accountability; and

Second, the elected and appointed officials of government would carry on their responsibilities within the context

of continuous, informed, and vigorous debate with the governed about actual and projected public policies. Democracy is pre-eminently government through open discussion.

4.3.5 FREEDOM OF INFORMATION AND PUBLIC ADMINISTRATION

McCamus (1981 : 5) states that the most crucial information imbalances are between the individual citizens under unfortunate circumstances and public authorities who have the power to give or withhold various forms of public assistance.

According to Trezza (1989 : 51) the citizen, in his daily interaction with public institutions should be entitled to know:

- a) Who, in fact, makes the decision about what concerns him;
- b) The legal source of power;
- c) The criteria, spelled out as explicitly as is practical according to which decisions are made;
- d) The factual information deemed relevant to the particular decision;
- e) The rationale of the decision; and
- f) The avenues of appeal against the decision.

In a democratic society, the citizens and their elected representatives should have access to this information upon which the decision of the government of the day to change the rules will be based. By the same token, one need to know what the effects of the prevailing rules have been so that they can be assessed, and, if necessary, changed (Trezza 1989 : 53).

4.3.6 RATIONALE FOR FREEDOM OF INFORMATION

According to Sieghart (1988 : 98) the rationale for freedom of information draws on a variety of strands. Access to information is the means by which the public can satisfy itself that those who act on its behalf are doing what they have promised; that what they have promised is feasible; and that the benefits claimed have occurred.

Openness is an essential safeguard against incompetence. It ensures that proposals are subject to scrutiny, mistakes are exposed and governments forced to learn from them. If a public authority is inefficient, negligent or complacent about matters requiring attention the mechanism that will ensure that it remains so is secrecy, the ability to cover its own tracks and conceal the consequences of its poor performance (Sieghart 1988 : 98).

Without information, people may be left in ignorance of developments directly affecting their communities, homes, jobs or amenities and deprived of the opportunity to express their views and influence the course of events. It is a safeguard against the arbitrary exercise of power, or its abuse for personal gain (Trezza 1989 : 61).

Sieghart (1988 : 99) states that the case for a right of access to information is compelling in relation to the personal files held by public authorities. An individual's file may be the basis on which benefits are offered or withheld; the need for services assessed, or penalties imposed on those believed to have transgressed. A right of access by the individual concerned provides the opportunity to ensure that the information is accurate and complete and allows the person to play a greater part in decisions about his own welfare.

4.3.7 CONTINUING STRUGGLE OVER CITIZEN ACCESS TO GOVERNMENT INFORMATION

Access to government information may have a valuable impact on a citizen's life. Not only may it help to prevent abuses of governmental power, it may also have more influence on the ordinary course of government decisions. Bureaucrats devote considerable time to prepare papers that are often called "memoranda for the

record" or "memoranda for file", documenting the reasons for their decisions and actions. To some extent this is merely good record-keeping, providing guidance for their successors and fellow workers. But these exercises in documentation are often also exercises designed to "cover" the bureaucrat in case of criticisms (Gordon and Heinz 1979 : xiv).

According to Marsh (1987 : 2) there are two reasons why the citizen of a democracy ought to be informed about the operations of the government:

First, it is feared that any government, if it is allowed to work in secrecy, will abuse the power entrusted to it; and

Second, the openness of the governmental process is essential to good government.

Jeremy Bentham (in Leigh 1980 : 30) notes that secrecy is an instrument of conspiracy and should never be a system of regular government. According John Stuart Mill (in Marsh 1987 : 2) the proper function of a representative assembly is:

To watch and control the government; to throw the light of publicity on its acts; to compel full exposition and

justification of all of them which anyone considers questionable; to censure them if found condemnable, and, if the men who compose the government abuse their trust, or fulfil it in a manner which conflicts with the deliberative sense of the nation, to expel them from office. Secrecy shields the abuse of office that endangers freedom and peace. Knowledge is power, in the familiar phrase. But secret knowledge is greater. It is the key to absolute power.

According to Woodrow Wilson (in Leigh 1980 : 33):

Everybody knows that corruption thrives in secret places, and avoids public places, and we believe it is a fair presumption that secrecy means impropriety. Secrecy as to its knowledge and intentions was a characteristic feature of any bureaucracy, whereby it seeks to increase the superiority of the professionally informed: The concept of the "official secret" is the specific invention of bureaucracy and it defends nothing so fanatically as this attitude.

The withholding of information and the power to release information at an opportune moment, are very powerful weapons in the hands of the politician in office, and his staying in office may indeed depend on the maintenance of that power (Riley and Relyea 1983 : 22).

One justification for public access to government-held information, is to redress the disequilibrium between the State and the individual, from whom information of all kinds is demanded by the State, and from which, information can only be obtained with difficulty, or not at all (Riley and Relyea 1983 : 22).

A second reason which is advanced in favour of the relaxation of government secrecy is simply that it is of the essence of democratic government that the public should have the right to be informed of the circumstances in which decisions are being taken in their name and at least have an opportunity to express their views, and that the quality of those decisions will be improved not only by the public's contribution to the decision-making process but even more by the knowledge of the decision-makers that are acting in the public view (Riley and Relyea 1983 : 22).

According to James Madison (in Riley 1986 : 17)

Knowledge will forever govern ignorance. And a people who mean to be their own governors must arm themselves with the power knowledge gives. A popular government without popular information, or the means of obtaining it, is but a prologue to a farce or a tragedy or perhaps both.

According to the Fulton Committee (in Horn and Gruber 1990 : 88) :

We think that the administrative process is surrounded by too much secrecy. The public interest would be better served if there were a greater amount of openness. The increasingly wide range of problems handled by government and their far-reaching effects on the community as a whole demand the widest possible consultation with its different parts and interests.

Teft (1980 : 54) asserts that government secrecy enables political leaders or government departments to cover up mistakes and violate laws in the interests of political and economic expediency. Secrecy also enables political leaders to conceal the fact that their political decisions were made to further personal interests or those of political allies at the expense of the public interest.

4.4 POLITICS AND SECRECY

Robertson (1982 : 182) is of the view that no Freedom of Information Act will give access to politics. No Freedom of Information Act will give access to the inner workings of political life. Governments know that they will not satisfy every member of the electorate, but this must not prevent them from taking decisions.

Teft (1980 : 67) states that all governments do not have the same degree of secrecy. The idea that secrecy is a boundary indicator is best summed up in the idea that it acts as the dividing point at which politics is said to cease and "reason" begin. Secrecy will cease at the point at which politics ends and reason begins. Politics is that part of political life in which politicians have the duty to determine what the aspirations and goals of society are.

4.4.1 NEED FOR GOVERNMENT SECRECY

Secrecy according to Lorch (1978 : 198) is viewed as being incompatible with democratic institutions. But it is very difficult to negotiate treaties or other agreements in public. The process of negotiation is usually more successful if done confidentially. There is a need for government secrecy.

Every person, body or institution is selective in the release of information. One often withholds information and conceals that part of one's lives which would be harmful if known. Concealment is also a major part of every administrator's work. Knowledge is power, and the power of every administrator is increased by his access to knowledge and by his ability to release that knowledge selectively to selected persons at selected times. Secrecy and selective release of information, are therefore, two

important tools of every administrator (Lorch 1978 : 198).

Horn and Gruber (1990 : 32) are of the opinion that every nation needs to keep secrets. Sensitive information used by diplomats, the military, and intelligence officers could harm the national interest if it became widely known.

The need to review the government's system of classifying information is pertinent to the discussion. Decisions to classify or to declassify information are important in a free society because they determine what information can and cannot, be made available to the public (Leigh 1980 : 38).

Horn and Gruber (1990 : 33) asserts that the "need to know" principle is one way to protect classified information. Too many people with clearances have access to too much information. A clearance should not entitle a person to anything. It is only one condition for use of classified material. Once an individual has met this condition, he should be given only that information he needs to know in order to do his job.

Classification decisions can be used to hide misconduct, to avoid public accountability, and to manipulate the public policy debate. For example the Department of Energy has known for some time that there were major environmental

problems at many of its nuclear weapons production facilities. Much of that information which was of importance for the public safety of those living nearby, was classified for years (Horn and Gruber 1990 : 33).

People in every society have to surrender some measure of personal liberty. Free societies are those in which the people retain the right to change their mind about how much freedom they are willing to sacrifice. But when people grant their government a licence to keep secrets, the right to change their mind is endangered (Horn and Gruber 1990 : 33).

According to Edward Shils (in Bulmer 1979 : 22)

Democracy requires the occasional participation of most of its citizenry some of the time and a moderate and dim perceptiveness - as from the corner of the eye - the rest of the time. It would not function if politics and the state of the social order were always in everyone's mind.

From the foregoing discussion it can be deduced that the relationship between the citizen and the government should be one of participation, trust, honesty and the free flow of ideas and knowledge.

4.4.2 COST OF FREEDOM OF INFORMATION AND SECRECY

Governments need to be concerned about the cost of freedom of information since every government service invokes the economic problem. Choices must be made between competing facilities and priorities must be set. The taxpayer has to bear the financial costs both directly and indirectly. Consequently these costs divert public resources from other services and from the provision of other benefits (Harrison 1980 : 57).

According to Horn and Gruber (1990 : 36) it is appropriate that the community should regularly pause to ask whether, the community is receiving value for money, in respect of the need for official information.

Riley (1986 : 7) states that information should flow freely in a country especially where that information concerns the operations of the political system and is the basis of decisions affecting many citizens. There are also countervailing considerations which limit the absolute right to know. Riley (1986 : 7) remarks:

Political accountability with individual authority in an age of large public administration engined by the new technology is what freedom of information is all about. Ultimately, it is about the distribution of

power in a modern state. Ultimately, it is a very modern issue of human rights, apt for recent times.

Freedom of information according to Rowat (1979 : 20) is a costly affair, in that a great deal of administrative labour is required to operate such legislation but it is also true that secrecy is expensive.

A hidden cost of secrecy is that much research and development is not available to other institutions or other scientists. This hampers the very development which governments are seeking. It is difficult to see how these fears and problems can be adequately discussed if research is being conducted in conditions of secrecy (Rowat 1979 : 21).

Another area in which secrecy has a cost to the public is the withholding of government investigations of public health, factory safety, drug safety and the reliability of consumer products (Leigh 1980 : 40).

Leigh (1980 : 40) states that a further argument against secrecy is that the taxpayer has paid for certain investigations to be carried out and is therefore entitled to the results. The more the government intervenes and the more information it demands from the public, the more it seems logical that the public should be entitled to receive

information from the government.

It can also be argued that the more active the government becomes, the more the public is in danger from government mistakes and therefore, the greater the need for public access to government information (Robertson 1982 : 190).

4.5 DEMOCRACY AND FREEDOM OF INFORMATION LEGISLATION

Riley (1986 : 85) states that freedom of information is sometimes confused with privacy protection laws. The simplest way to delineate the differences between the two is that the former deals with topical records held by government while the latter concerns one's own personal file which largely cannot be assessed by anyone else.

It is of vital importance that one recognises what kinds of information one would ever be able to obtain from any democratic government. One can never envisage a situation in which politicians would be forced to divulge what was in their minds by virtue of any piece of legislation. One cannot force politicians to state what they think they may do, and what is possible or impossible. In one sense it is impossible to prohibit secrecy (Riley 1986 : 85).

Openness then does not guarantee that the government will provide access to all of its thinking and information, but it does provide an incentive to the government to ensure that what the public does have access to is enough to protect itself. Without legislation providing for public access to government documents, and the incentive for the government not to provide half truths and lies is much less (Horn and Gruber 1990 : 40).

4.5.1 NEED FOR FREEDOM OF INFORMATION LEGISLATION

According to McCamus (1981 : 13) freedom of information legislation is needed to establish openness as a fundamental value in shaping the process by which one is governed. Openness, however, is not the overriding value in all circumstances.

Information in the possession of the government should be made available to those who want it outside the government (McCamus 1981 : 13).

The case for a Freedom of Information Act is not that all secrecy is wrong. All such Acts contain exemptions, for example, to protect the necessary defence or commercial secrets, personal privacy, information that would help criminals commit offences, or information that has to be kept secret during international negotiations if a credible

bargaining position is to be preserved. The government should be able to protect such information (Sieghart 1988 : 106).

Sieghart (1988 : 106) asserts that there should be a general right of access to official information, with exceptions allowed only where the government can show that information falls into one of the legally exempted categories. An independent right of appeal to the courts or an ombudsman are an essential component against false government claims.

A Freedom of Information Act would mean a substantial move toward more accountable government. Ministers and officials would be less able to conceal mistakes or get away with inaction on matters of pressing public concern. Proposals would be exposed to more effective scrutiny, and objections would be more difficult to ignore (Leigh 1980 : 43).

Therefore, freedom of information legislation guarantees the citizen a right of access to information, albeit with certain exceptions. It means that the citizen will be in a position, if he or she so chooses, to know what one's government is doing and why. It means that the citizen, who pays the taxes which finance the gathering of that information, will have the right to scrutinise the

information. There should be an opportunity for the electorate to be informed (Riley 1986 : 87).

Such a law, then, according to Riley (1986 : 88) implies that the government of the day shall be accountable for what it is doing and for the policies it implements in the name of the people it is governing. There are other forms of accountability for governments, such as parliamentary debates, parliamentary committees to which the executive are answerable, the media and, ultimately, the voting booth. An information law is an important cornerstone of the democratic process.

Information laws could also be described as being of help to government itself, for such statutes would give the people, a better understanding of government when citizens participate in the democratic process. More importantly, they would give the people the feeling that they do have some control over the actions of governments other than just every two-to-five years when they go to the polls, and thus increase their confidence in government (Sieghart 1988 : 107).

According to Gerald Baldwin, founder of the International Freedom of Information Institute, this type of law is critical. He said (in Delbridge and Smith 1982 : 32):

People are tired of the old ways of government, with the problems of inaccessibility, growing inflation, a burgeoning bureaucracy and many other problems. I am convinced that what is needed is more accountability of governments, which would include good information laws, or people are going to throw away the current institutions and replace them with something far worse. The time for governments to act and to take up their responsibility is now.

The biggest beneficiary of all is the citizen, the individual on whose day-to-day life the major policy decisions of government have such an impact (Riley 1986 : 90).

What an Information Act means according to Riley (1986 : 90) is that pertinent information in the areas of education, health, housing, the environment and other sectors of daily life can become available. A Freedom of Information Law which pays lip service to the access principle is a disservice to the people and highlights the necessity to educate the citizenry about the rights which exist in access legislation.

In the words of Lord Acton (in Riley and Reylea: 1983 : 28)

Everything secret degenerates, even the administration of justice; nothing is safe that does not show it can bear discussion and publicity.

4.5.2 EXCLUSIONS, ENFORCEMENTS AND OTHER CONSIDERATIONS

One of the crucial elements in any freedom of information legislation is the exclusions question, that is, what categories of information are public authorities to be permitted to withhold from the public? Such legislation should include exclusions in precise and detailed terms (McCamus 1981 : 15).

4.5.3 SPECIFIC LIMITATIONS ON ACCESS

A detailed analysis on information which is exempted from public access is discussed below.

(a) MAIN EXEMPTIONS FROM ACCESS

The most commonly accepted exemptions from any right of access, as noted in Marsh (1987 : 7) relate to information:

- (i) the disclosure of which is prohibited by statutory provisions preceding the legislation providing for the right of access;

- (ii) Which has come into the possession of the government before a certain date (such as the date when the legislation introducing the right of access was passed);
- (iii) concerning international relations and national security;
- (iv) concerning law enforcement and the prevention of crime;
- (v) concerning discussions, advice given, or opinions expressed within the government organization;
- (vi) which has been obtained in confidence from a source outside the government organization;
- (vii) which, if disclosed, would violate the privacy of an individual;
- (viii) which (being generally of an economic character) would, if disclosed, or disclosed prematurely, confer an unfair advantage on some person or inflict an unfair disadvantage or injury on either the government or some other person; and

(ix) which is covered by legal professional privilege.

**(b) EXEMPTION OF LEGISLATION CONCERNING INTERNATIONAL
RELATIONS AND NATIONAL SECURITY**

A government in a democratic society is ultimately responsible to the electorate for its conduct in the handling not only of domestic but also of international affairs and national security (Horn and Gruber 1990 : 45).

Marsh (1987 : 8) asserts that governments still argue:

- (1) that in international relations there is as yet no common acceptance of open diplomacy in all circumstances;
- (2) that each government is responsible for the national security of its country, which necessarily involves a measure of secrecy as to its own defence forces and their plans, and as to the protection of that secrecy by counter-espionage, as well as to the espionage it undertakes to ascertain the extent of any threat to that security from other countries;
- (3) that information which a citizen might reasonably demand of his own government cannot in practice be

disclosed without becoming internationally available and thereby an embarrassment in its dealings with other governments and possibly a danger to the national security for which it is responsible; and

- (4) that only a national government which has the day-to-day experience of conducting international relations can judge when disclosure of information in its possession concerning international relations or national security is justified.

The activities of a government in the international field are of importance to the citizen above all those which may affect the issues of peace and war. This idea is shared by Thomas Jefferson (in Trezza 1989 : 54) as follows:

It is in their sweat which is to earn all the expense of the war and their blood which is to flow in expiation of the causes of it especially when that war may be of the nuclear kind. Yet the citizen cannot properly pass judgement on those activities unless he has the means of informing himself about them and the circumstances in which they are pursued. Of all the exemptions from access, that concerning international affairs and national security is one of the most keenly debated and one where it is most difficult to reach equilibrium between the claims for secrecy and the

demands of the public for disclosure.

(c) EXEMPTION OF INFORMATION WHICH, IF DISCLOSED, WOULD VIOLATE THE PRIVACY OF AN INDIVIDUAL

According to Warner and Stone (1974 : 56) information which is exempted from public access because it had been obtained in confidence from a source outside the government may well include information which, if disclosed, would violate an individual's privacy.

There is a need to provide an exemption from access to cover individual privacy. For example, documents in a government's possession may show that a particular individual is suffering from cancer. Whether that is a matter to be treated as private to him will depend on a number of factors; for instance, he is a man in public life whose capacity to fill a particular appointment would be questionable if he had such an illness, then the exemption from access would not be justified. Although the concept of privacy remains the extent to which it may be affected by elements of public interest can vary between countries and from age to age (Warner and Stone 1974 : 57).

In addition, what a man earns or what he leaves in his will according to Young (1978 : 245) may be regarded as typically private information in one country whereas in

another it may be considered as knowledge in which the public have a proper interest.

(d) EXEMPTION OF INFORMATION (GENERALLY OF AN ECONOMIC CHARACTER) WHICH, IF DISCLOSED, OR DISCLOSED PREMATURELY, WOULD CONFER AN UNFAIR ADVANTAGE ON SOME PERSON, OR WOULD SUBJECT SOME PERSON, OR THE GOVERNMENT TO AN UNFAIR DISADVANTAGE.

According to Marsh (1987 : 18) a Budget Secret would be an example of information which, if known to unauthorized persons prematurely, may confer an unfair advantage on them and cause disadvantage to others.

Governments are especially concerned to keep economic information to themselves, not because its release would necessarily involve unfairness under discussion but because they would prefer to pursue their economic activities with as little outside criticism as possible (Marsh 1987 : 18).

4.5.4 PUBLICATION OF DOCUMENTS BY THE GOVERNMENT

Sieghart (1988 : 188) states that it is much more convenient for the government itself to publish documents, which the citizen seeks.

The business of modern government is complicated and of a diverse nature. According to Trezza (1989 : 161) what is needed prior to the introduction of any scheme of public access to government held information, is an educational programme for the benefit of the administrator and the ordinary citizen (Trezza 1989 : 161).

4.5.5 SCOPE OF PUBLIC INSTITUTIONS COVERED BY THE ACCESS LEGISLATION

It will be found that the systems of public access relates to the central government and the departments which it controls. It is important to emphasise that, if public access to information gives the individual citizen a more meaningful role in the control of governmental decisions, public access should apply to all levels of democratic government i.e. central, regional and local level (Harrison 1988 : 90).

Harrison (1988 : 90) is of the view that a degree of "openness" at the local level of government may be in the interests of the central government, which would be hesitant to accept public access to information in its own keeping.

4.6 SUMMARY

The United Nations endorses freedom of information as a fundamental human right. Freedom of information implies the right to publish information and the free flow of information without undue government restrictions. It means the right to inform the public without being fettered by regulations which in any way restricts this right. In another context, it has come to mean the free flow of information across borders unfettered by government regulations.

The objective of a public right to know is the prevention of the manipulation of information and to give substance to the democratic requirement of accountability. Access to information is the means by which the public can satisfy itself that those who act on its behalf are doing what they have promised. It further creates a citizenry which is active, knowledgeable and lively.

Without a legal right to freedom of information, government will be able to manipulate information for its own ends, mainly to preserve itself in office, releasing only that information which is to their credit or undermines the credibility of their opponents.

Government secrecy produces apathy and ignorance. This state of affairs is dangerous to democracy since they produce a citizenry who will be unable to participate in political life. However, there is some need for official secrecy for purposes of national security.

Every person, body or institution is sensitive in the release of information and government is no exception. Every nation needs to keep secrets.

There can never be a right to know all that a citizen might like to know. There can only be a right to know certain specified and carefully defined types of information.

It is simpler and more convenient if the government takes the responsibility for publishing the documents that the citizens seeks. Public access to information should apply at all levels of government viz., central, regional and local levels.

For the taxpayer, freedom of information is a costly exercise but it is true that secrecy is more expensive.

CHAPTER 5

TRENDS IN INFORMATION PRIVACY PROTECTION AND PROMOTION OF FREEDOM OF INFORMATION : INTERNATIONAL AND NATIONAL PERSPECTIVE

Information is the currency of democracy.
The sword of democracy is blunted
by the indifferent voter
who is ignorant about what is
going on in his country

Anon

5.1 INTRODUCTION

Concern for the protection of personal privacy is a pressing issue in western democracies as individuals are increasingly subject to surveillance by government and data banks (Hondius 1975 : x).

According to Flaherty (1989 : 13) individuals want to be left alone to exercise some control over how information about them is used. Legislators have responded to widespread fears about the impact of computers on personal privacy by enacting protective laws. These measures seek to control the government's collection, use, and dissemination of personal information by means of codes

or fair information practices. The issue is whether such data protection laws and the institutions created to implement them have been effective watchdogs in limiting governmental surveillance of the population and in promoting bureaucratic accountability in data use.

The focus of the first part of this chapter is on an evaluation of the accomplishments in controlling surveillance by the officials charged with protecting certain aspects of personal privacy in the Federal Republic of Germany, Sweden, France, Canada, and the United States. The countries selected for treatment illustrate the leading approaches to data protection (Flaherty 1989 : 15)

The second part of this chapter concentrates on freedom of information.

Baxter (1984 : 234) states that access to certain official information is a necessary prerequisite for public accountability and an essential feature of modern democratic theory. Even at the level of administrative decision-making it is important that persons who may be affected by administrative action should have access to the information upon which the public authority relies. This is essential if they are to make effective representations or if they are to evaluate the ultimate decision rationally. Without this facility, those who suffer

disadvantage as a result of a decision are hardly likely to regard it as fair, nor are they likely to have confidence in the administrative process.

5.2 INFORMATION PRIVACY AND FREEDOM OF INFORMATION LAWS

Privacy or data protection laws are sometimes confused with freedom of information laws. It is necessary for the purpose of this discussion to distinguish between information privacy and freedom of information laws (Riley 1986 : 85).

According to Sloan (1986 : 198) the right to have access to one's own personal file, the right of correction, and the right to have that information kept in a certain manner, are referred to as "fair information practices". These rights are called Privacy Acts in some countries and Data Protection Acts in others.

Riley (1986 : 85) states that freedom of information or access legislation guarantees the citizen a right of access to information, albeit with certain exemptions. It means that the citizen will be in a position, if he or she chooses, to know what one's government is doing and why. It means that the citizen who pays the taxes which finance the gathering of that information, will have the right to scrutinise the information. There would exist an

opportunity for an electorate to be informed of governmental affairs.

5.3 INFORMATION PRIVACY LEGISLATION :

INTERNATIONAL PERSPECTIVE

In this section it is necessary to delve into the question of why nation-states require information protection laws in the information age and how best to protect personal privacy. The Federal Republic of Germany and Canada use an advisory model, while Sweden and France have regulatory and licensing approaches (Hondius 1975 : 12).

An effort is being made in this section to reach an adequate comprehension of personal privacy protection in South Africa.

5.3.1 FEDERAL REPUBLIC OF GERMANY

Flaherty (1984 : xv) asserts that the European and Canadian Data Protection Commissioners and protection departments function as spokesmen for privacy and data protection interests in their respective statutory spheres. The German system of data protection has particular relevance for the federal systems of government that exist in North America. The Federal Data Protection Act in Germany became law on 27 January 1977. Its detailed principles for data

protection in the public sector are comparable to the principles of fair information practices usually incorporated in such laws. Significantly, Germany has a co-ordinated system of implementation in place for the Federal and State Data Protection Acts. Each of the eleven states and the federal government has its own Data Protection Commissioner or Commission. The German data protection laws give heads of government departments the primary responsibility for their implementation.

According to the International and Comparative Law Quarterly (1992 : 171) Germany is a law-driven society, and every civil servant acknowledges a direct legal responsibility to implement data protection.

5.3.1.1 APPOINTMENT OF THE FEDERAL DATA PROTECTION COMMISSIONER

The German federal data protection statute requires the appointment of a Federal Data Protection Commissioner. The Data Protection Commissioner serves a five year term and is independent in performing his duties. The degree of independence from the government is an important characteristic of this office (Bull 1981 : 9).

5.3.1.2 DUTIES OF THE FEDERAL DATA PROTECTION COMMISSIONER

According to Bull (1981 : 9) the duties of the Data Protection Commissioner are to ensure that the provisions of the Data Protection Act are implemented in the federal public sector. He may make recommendations for the improvement of data protection and may give advice to the federal government and individual ministers. He is required to present an annual activity report to the legislature, which is one of his main ways of highlighting any problems in the implementation of data protection.

If the Federal Data Protection Commissioner discovers "infringements against the provisions of this Act, against other data protection regulations, or other irregularities in the processing of personal data", he can submit a complaint to the relevant authority; thus his power is only advisory. Such advice has been taken very seriously by federal authorities (Flaherty 1984 : xvi).

It is not politically viable for the heads of federal departments to ignore the advice of the Data Protection Commissioner. The office only issues public statements when fundamental differences of opinion occur or breaches of the data protection law have been found during an audit or inspection. The Federal Data Protection Commissioner's office also receives complaints from individuals, who

identify possible problems (Flaherty 1984 : xvi).

5.3.1.3 STAFF OF THE FEDERAL DATA PROTECTION COMMISSIONER

Bull (1981 : 11) states that the Office of the Federal Data Protection Commissioner has a staff of about thirty-five persons, at least half of whom are professionals (mainly persons with academic training in law).

This staff specializes in various types of federal information systems since data protection is complicated in its application and has to be adapted to the particular needs of each system (Bull 1981 : 11).

A primary goal of all the German data protection offices according to Flaherty (1984 : xvii) is to see that specialized data protection provisions are incorporated in the detailed laws governing each type of information-handling activity in the public sector. This particular activity is a central goal of data protection; it requires the consistent application of expertise on behalf of privacy interests.

The first six years of the implementation of data protection in Germany, especially at the federal level, have been very successful. With Professor Hans Peter Bull

as the first federal Data Protection Commissioner from 1978 to 1983, the data protectors learned a great deal about the real state of data processing and data communication. Even though the office does not have the power to give direct orders, this has not hindered the successful conduct of data protection to date (Flaherty 1984 : xvii).

The Federal Data Protection Office seems to have done its work without any major breakdown in its relationship with the subjects of regulation. The annual activity reports of the Office are full of illustrations of progress achieved, even if many specific problems continue to exist. In many ways the various data protectors at the federal and state levels have successfully engaged in a very active programme of informing the public, and the general public has supported their efforts (Flaherty 1984 : xvii).

5.3.1.4 CHRONOLOGY OF GERMAN DATA PROTECTION LEGISLATION

Data Protection Legislation in Germany commenced at the beginning of the 1970's when the State of Hesse enacted a Data Protection Act. In 1977 the Federal Data Protection Act was enacted. Various amendments were made to this Act during the course of the years and is still existent today. (Flaherty 1984 : xvii). The chronology of German Data Protection Legislation is presented in Table 5.1.

TABLE 5.1 : CHRONOLOGY OF GERMAN DATA PROTECTION LEGISLATION

1969	Social Democratic Party hold national power.
1970	State of Hesse enacts a Data Protection Act.
1973	Federal Ministry of the Interior presents a draft bill on data protection to the Bundestag.
1975	Spiros Simitis becomes Data Protection Commissioner for the state of Hesse.
1977	Federal Data Protection Act (BDSG) enacted.
1978	Hans Peter Bull becomes Federal Data Protection Commissioner.
1979	Heinrich Weyer becomes Data Protection Commissioner for the state of North Rhine-Westphalia.
1982	Helmut Kohl, a Christian Democrat, replaces Social Democrat Helmut Schmidt as chancellor.
1983	Reinhold Baumann becomes Federal Data Protection Commissioner.
1986	Hesse revises its Data Protection Act.
1988	North Rhine-Westphalia revises its Data Protection Act. Alfred Einwag becomes Federal Data Protection Commissioner.

(Flaherty 1989 : 23).

5.3.2 SWEDEN

According to Freese (1981 : 3) Sweden was the first country to pass a national data protection law with its Data Act of 1973. It required the licensing of all personal registers in both the public and private sectors and compliance with a set of strict standards to prevent unwarranted invasion of privacy. The statute was amended to the present Data Act of 1982 which seeks to reduce the bureaucratic burden of data protection and to make the new system of selective licensing of personal information systems and self-supporting.

5.3.2.1 DATA INSPECTION BOARD

Jan Freese, the Director General of the Data Inspection Board, performs a crucial role as a publicist and activist for data protection in Sweden and elsewhere. He took the initiative to educate the people on their right to privacy, warning them about the consequences of record linkages, and highlighting the extent to their country is already a paradise for data banks. Freese is regarded as the model for activist data protectors (Flaherty 1984 : xvii).

5.3.2.2 STAFF OF THE DATA INSPECTION BOARD

The staff of the Data Inspection Board is overloaded with

work, because of the large numbers of automated personal registers in the public and private sectors (Flaherty 1984 : xvii).

The staff of less than thirty persons at the Data Inspection Board cannot implement data protection effective in both the public and private sectors. Annual charges for licences have not generated enough income to make the Data Inspection Board financially self-supporting. The staff are resistant to becoming bill collectors as opposed to data protectors. The bureaucratic burden of trying to collect annual license fees from users clearly detracts from data protection activities (Flaherty 1984 : xviii).

The state of data protection in Sweden after more than a decade of experience raises some interesting questions. The issue has lost some of its novelty and political support. Over time, this poses a critical problem for data protection departments in every country (Flaherty 1984 : xviii).

5.3.2.3 CHRONOLOGY OF SWEDISH DATA PROTECTION LEGISLATION

The Data Act of 1973, the first national law on data protection, has had a considerable influence on the development of statutes in other Western European countries. The Data Inspection Board focuses on the

nature and quantity of personal data collected, how and from whom the data are acquired. In 1982 there were major amendments to the Data Act (Flaherty 1989 : 93). The chronology of Swedish Data Protection Legislation is presented in Figure 5.2.

TABLE 5.2 : CHRONOLOGY OF SWEDISH DATA PROTECTION LEGISLATION

1973	Data Act enacted. Data Inspection Board (DIB) begins operation with Claes-Goran Kallner as director general.
1976	Parliamentary Commission on Revision of the Data Act (DALK) created.
1977	Jan Freese becomes Director General of the DIB.
1978	Parliamentary Commission on Revision of the Data Act issues a major report.
1980	Secrecy Act amended.
1982	Major amendments to the Data Act.
1983	Major amendments to the Data Act enter into effect.
1986	Mats Borjesson becomes Director General of the DIB.
1988	Re-election of the Social Democrats.

(Flaherty 1988 : 97).

5.3.3 FRANCE

According to Tapper (1992 : 11) the French Data Protection Law of 6 January 1978 on Informatics and Freedoms is expansive and innovative.

5.3.3.1 NATIONAL COMMISSION ON DATA PROCESSING AND FREEDOMS (CNIL)

Provision is made in the Data Protection Act, for the creation of an independent administrative authority with regulatory power, the National Commission on Data Processing and Freedoms (Flaherty 1984 : xviii).

5.3.3.2 STAFF OF THE NATIONAL COMMISSION ON DATA PROCESSING AND FREEDOMS (CNIL)

This Commission has seventeen (part-time) members chosen for five-year terms from various groups, courts, and legislative bodies. They give advice to the government on the authorization of particular personal information systems. When the first five-year terms ended in 1983, seven new members joined the Commission. The Commission has several politicians as commissioners (Tapper 1992 : 12).

According to Flaherty (1984 : xviii) the limited effectiveness of the Commission in its first five years

suggests some of the problems of depending on part-time Commissioners for strong implementation of data protection.

Tapper (1992 : 14) is of the view that successful data protection requires talented and committed professional staff in all countries.

Critics argue that the Commission has never taken a tough decision against the government with respect to a proposed new personal information system. It has also not reviewed in detail all of the personal databanks that existed prior to the enactment of the 1978 law and has concentrated on reviewing the creation of new systems (Flaherty 1989 : 192).

According to Tapper (1992 : 15) French data protection has yet to reach the level of maturity and accomplishment of its German and Swedish equivalents.

5.3.3.3 CHRONOLOGY OF FRENCH DATA PROTECTION LEGISLATION

The Tricot Commission was appointed in 1974. This Commission concluded that preventive action was necessary to reduce the serious potential for abuse of computers. The government then proposed a Law on Informatics and Freedoms (Flaherty 1989 : 167). Further amendments on

this law were made and is still in force today. The chronology of French Data Protection Legislation is presented in Table 5.3.

TABLE 5.3 : CHRONOLOGY OF FRENCH DATA PROTECTION LEGISLATION

1974	Ministry of Justice appoints Commission on Informatics and Liberties (Tricot Commission). Commission submits its report.
1976	Government proposes a law on Informatics and Freedoms.
1978	Enactment of the Law on Informatics and Freedoms. Entry into force of the Law on Informatics and Freedoms. Appointment of the first members of the CNIL and election of Pierre Bellet as the first president.
1979	Jacques Thyraud elected president of the CNIL.
1981	Francois Mitterrand elected President of France.
1983	Five-year terms of office - members of the CNIL. Jean Rosenwald elected president of the CNIL.
1984	Jacques Fauvet elected president of the CNIL.
1988	Mitterrand elected president of France for a second term. Five-year terms of office of the members of the CNIL renewed (six new members). Jacques Fauvet re-elected president of the CNIL.

(Flaherty 1989 : 167).

5.3.4 UNITED KINGDOM

In 1982 the government of Prime Minister Margaret Thatcher committed itself to go forward with data protection legislation. A Data Protection Bill was passed by the House of Lords in March 1983, where it was re-introduced in modified form on 23 June after the general election. The Bill is a complex piece of legislation that establishes an independent Data Protection Registrar with a proposed staff of twenty to thirty non civil servants, who will register all users of automated personal information systems in the public and private sectors (Milmo 1993 : 1182).

Schedule I of the Data Protection Bill sets forth data protection principles ; the task of the Registrar will be to ensure that all data users comply with fair information practices in their uses of personal data (Flaherty 1984 : xix).

The Registrar may refuse to register a data user, if he or she is satisfied "that the application is likely to contravene any of the data protection principles". Data subjects have the right to be informed that data about them are being collected, and the right to sue for damages if their data are disclosed without authority. An appeal is possible from a decision of the Registrar to the newly

created Data Protection Tribunal and, ultimately, to the courts (Milmo 1993 : 1183).

5.3.5 CANADA

According to Onyshko (1989 : 213) the relevant data protection legislation in Canada is the Federal Privacy Act of 1982, which supplanted and significantly strengthened the privacy provisions in Part IV of the Canadian Human Rights Act of 1977. The latter introduced statutory principles of fair information practice in the federal public sector and also created the post of Privacy Commissioner. The tasks of the Commissioner consisted primarily of responding to complaints from individuals.

5.3.5.1 PRIVACY COMMISSIONER

The Federal Privacy Law of 1982 according to the Report of the Privacy Commissioner (1982 : 127) strengthened the general powers of investigation and monitoring and set up an Office of the Privacy Commissioner, separate from the Canadian Human Rights Commission. The Privacy Act regulates the collection, retention, disposal, protection, and disclosure of personal information by the federal government. Aggrieved individuals can bring complaints to the Privacy Commissioner. Denials of requests from persons for access to their personal information can be taken

to the Federal Court of Canada.

The Privacy Commissioner and his staff have to act affirmatively to make the law truly effective. Successful implementation will require such positive initiatives on the part of the Privacy Commissioner as carrying out supervision, audits, and inspections of federal personal information practices (Onyshko 1989 : 214).

5.3.5.2 DEVELOPMENTS IN CANADIAN DATA PROTECTION

Quebec is the only province in Canada that has enacted data protection legislation for the public sector, setting up a commission along the lines of existing European data protection models. Quebec passed Law 65 in June 1982 on the basis of the recommendations of the Pare report in 1981 (Report of the Privacy Commissioner 1982 : 130).

The three members of the independent supervisory Commission d'Access a l'Information, whose responsibilities include overseeing the protection of privacy in the public sector, were appointed by the National Assembly in December 1982. The Quebec Law incorporates the provisions for fair information practices usually found in data protection laws. Thus personal data collected by a public body have to be necessary, accurate, timely, and complete (Onyshko 1989 : 214).

The primary need in Canada is for the nine provinces without general data protection legislation in the public sector to take steps to fall in line with developments elsewhere. To date, the federal government and Quebec have taken the novel approach of integrating laws on privacy and access to general government information. This helps to avoid some of the conflicts which have arisen between the Freedom of Information Act and the Privacy Act in the United States (Onyshko 1989 : 216).

5.3.5.3 CHRONOLOGY OF CANADIAN DATA PROTECTION LEGISLATION

A Task Force on Privacy and Computers was established in the early 1970's. Thereafter the federal government set up an Interdepartmental Committee on Privacy in order to prepare a law for the federal government. In 1978 the Canadian Human Rights Act came into existence. In the early 1980's Privacy and Access to Information Acts were introduced (Flaherty 1989 : 244). The chronology of Canadian Data Protection Legislation is presented in Table 5.4.

TABLE 5.4 : CHRONOLOGY OF CANADIAN DATA PROTECTION**LEGISLATION**

1972	Publication of Privacy and Computers by the Task Force on Privacy and Computers.
1975	Interdepartmental Committee on Privacy, chaired by the Department of Justice and Communications, produces draft legislation.
1976	Liberals introduce Bill C-25, the Canadian Human Rights Act, a revised version of Bill C-72.
1977	Bill C-25, the Canadian Human Rights Act, receives royal assent. Inger Hansen appointed Privacy Commissioner.
1978	Bill C-25, the Canadian Human Rights Act, proclaimed in force.
1980	First reading of Bill C-535, the Privacy Act, 1980 introduced as a private member's bill by Conservative M P Perrin Beatty. Liberals introduce Bill C-43, to enact the Access to Information Act and the Privacy Act.
1982	Bill C-43 receives royal assent.
1983	John Grace appointed Privacy Commissioner. Access to Information Act and Privacy Act proclaimed in force.

(Flaherty 1989 : 244).

5.3.6 UNITED STATES OF AMERICA

According to the Report of the United States Privacy Council and Computer Professionals for Social Responsibility (1991 : 1) the United States has a rapidly developing body of law for the protection of personal privacy. However federal and state achievements in data protection are somewhat limited when compared to European standards.

5.3.6.1 PRIVACY ACT OF 1974

The Privacy Act of 1974, the second national law of this type after Sweden's, mandated fair information practices for the federal government, which collects billions of items of personal data. The Privacy Act had a major initial impact but, unfortunately, it has a major structural flaw in terms of effective implementation (Flaherty 1989 : 305).

In the entire United States federal government there is no single body of independent officials charged with articulating and defending the privacy interests of citizens on a continuing basis. As new ideas for monitoring the population are brought forward by the executive and legislative branches, there is no one formally charged with evaluating their implications for

personal privacy. The contrast with the situation in Germany, France, Sweden and Canada is striking (Report of the United States Privacy Council and Computer Professionals for Social Responsibility 1991 : 5).

5.3.6.2 PRIVACY PROTECTION STUDY COMMISSION

In lieu of an oversight agency, the Privacy Act created a Privacy Protection Study Commission, which produced a comprehensive report in July 1977 on Personal Privacy in an Information Society. It remains the best overall analysis of the data protection needs of various types of personal information systems in both the public and private sectors (Report of the United States Privacy Council and Computer Professionals for Social Responsibility 1991 : 5).

Legislative measures for data protection have to be revised on a continuing basis in response to new challenges from information technology (Flaherty 1984 : xxi).

5.3.6.3 CHRONOLOGY OF UNITED STATES FEDERAL DATA PROTECTION LEGISLATION

A Freedom of Information Act was enacted in 1966. In the early 1970's there were major amendments to the Freedom of Information Act and the Privacy Act of 1974 came into existence. The Privacy Protection Study Commission was

appointed in 1977. This Commission provided valuable information on the protection of personal privacy. In the early 1980's the protection of privacy continues to be a pressing concern (Flaherty 1989 : 306). The chronology of United States Federal Data Protection Legislation is presented in Table 5.5.

TABLE 5.5 : CHRONOLOGY OF UNITED STATES FEDERAL DATA PROTECTION LEGISLATION

1966	Freedom of Information Act enacted.
1974	Major amendments to the Freedom of Information Act. Senator Samuel J Ervin Jnr introduces S.3418 to create a Federal Privacy Board. President Ford signs the Privacy Act.
1975	Department of Defence creates the Defence Privacy Board. Office of Management and Budget issues guidelines on the implementation of the Privacy Act. Privacy Act enters in force.
1977	Report of the Privacy Protection Study Commission.
1978	Right to Financial Privacy Act regulates federal access to individual financial records.

1979	Office of Management and Budget issues guidelines for the conduct of matching programmes.
1980	Office of Management and Budget creates the Office of Information and Regulatory Affairs.
1982	Office of Management and Budget issues revised supplemental guidelines for conducting computer matching programmes.
1983	Congressman Glenn English chairs the first oversight hearings of the Privacy Act.
1986	Office of Technology Assessment issues a report on "Electronic Record Systems and Individual Privacy".
1987	House of Representatives holds hearings on computer matching legislation.
1988	Computer Matching and Privacy Protection Act enacted to control computer matching.

(Flaherty 1989 : 307-8).

5.4 INFORMATION PRIVACY LEGISLATION : **NATIONAL PERSPECTIVE**

Attention is now focused on developing a model of information privacy for South Africa.

5.4.1 SOUTH AFRICA

McQuoid-Mason (in Bayat and Sing 1994 : 365) writing on the adequacy of the past South African Law in protecting information privacy, states:

South African Law has been unable to safeguard the individual adequately against the collection of information in data banks by the public and private sectors. While the common-law remedies may be adequate once the individual discovers that he has become the subject of an offensive invasion of privacy, in most cases he is not aware that his privacy has been invaded.

Section 13 of the Republic of South Africa Constitution Bill, 1993 makes provision for the right of privacy as a fundamental right:

Every person shall have the right to his or her personal privacy, which shall include the right not to be subject to searches of his or her person, home or property, the seizure of private possessions or the violation of private communications.

5.4.1.1 MEASURES TO PROTECT INFORMATION PRIVACY RIGHTS

Any legislative measure to protect and promote the information privacy rights of the individual should take cognisance of the following aspects discussed in the Report of the Privacy Committee of New South Wales (1991 : 42-47):

(i) SCOPE AND APPLICATION

The principal objective should be the protection of information privacy. Attention should be focused on whether legislation should apply to the public sector or to the private sector as well.

(ii) DEFINITIONS

Attention must be given to the most important definition, i.e. that of "personal information". Should the definition include, for example, biographical information, employment information, information on financial affairs, medical information, information on leisure activities, travel information, ideological information?

(iii) INFORMATION PROTECTION PRINCIPLES

The principles should be the hallmark of the legislation. The success of the legislation will depend on how these principles are formulated.

The principles should address the following matters:

- manner and purpose of collection of personal information;
- collection of only the necessary information from the record subject;
- informed consent;
- storage and security of records of personal information;
- information relating to records of personal information;
- access to records containing personal information;
- rectification, notation and erasure of records;
- use and disposal of records of personal information;

- limits on use of records of personal information;
and
- limits on disclosure of records of personal information.

(iv) CODES OF PRACTICE

Provision should be made for the development of codes of practice in respect of specific types of records and new forms of technology. Codes of Practice can be used to provide information protection standards to the activities and needs of different sectors. For example, in the government sphere of operation, codes could be developed in relation to medical records and research and police records.

(v) COMPUTER MATCHING AND DATA LINKAGE

Programmes that involve data matching should be reported to the Privacy and Information Protection Ombudsman with a statement describing:

- the type of information to be matched;
- the source of the information; and
- the purpose of the match.

(vi) TRANSBORDER DATA FLOWS

Legislation should address the issue of transborder data flows by requiring that data be transferred out of a country only when the transfer is required by law or treaty, or when the receiving party can ensure equivalent data protection.

(vii) ENFORCEMENT, OFFENCES AND REMEDIES

Legislation should create a limited range of offences for the most serious and wilful breaches of information privacy protection principles.

Individuals should be able to obtain compensation for damage suffered as a result of the breach of particular data protection principles (e.g. damage arising from unauthorised disclosure of personal information).

**(viii) ESTABLISHMENT OF AN OFFICE OF THE PRIVACY AND
INFORMATION PROTECTION OMBUDSMAN**

Provision for funding this office should be contained in statutory legislation.

(a) FUNCTIONS AND POWERS OF THE OMBUDSMAN

The ombudsman should be given advisory and investigative powers.

The types of functions performed by the Ombudsman should include:

- the promotion of compliance with the information privacy protection principles by public and private sectors;
- the supervision of compliance with the information privacy protection principles by public and private sectors;
- the investigation of complaints alleging breaches of the information privacy protection principles;
- the investigation of complaints alleging interferences with privacy of persons;
- the conduct of research in respect of any matter relating to the privacy of the person;
- the provision of advice to any person and preparation and publication of reports and

recommendations concerning the need for, or desirability of legislative, administrative or other action in the interest of the privacy of persons;

- the preparation and publication of guidelines to promote the protection of privacy; and
- the monitoring of developments in technology which may have an adverse impact on the privacy of persons and the preparation of reports on how any adverse impact may be minimised.

The Ombudsman's powers should include:

- the powers necessary to conduct investigations and inquiries including the power to summon witnesses, to administer oaths;
- to enter premises, examine and obtain copies of documents, and to examine recordkeeping systems;
- the power to audit public sector authorities to determine whether they are complying with the information privacy protection principles including

the power to audit records exempt from access by the record subject;

- the power to make public statements; and
- the power to make special reports to Parliament.

(ix) REVIEW BY THE LEGISLATURE

Provision should be made for the establishment of a parliamentary joint committee to monitor and review the ombudsman's exercise of his powers and functions.

(x) PROVISION OF TECHNOCRATS AND PERSONNEL

Legislation should make provision for the Ombudsman to obtain expert assistance for the purposes of the conduct of inquiries, investigation and research. The type of assistance required may be expertise in computer technology and information systems, medical practice and procedure and so on. Personnel should also be employed to assist the Ombudsman in the performance of his daily duties and be under the control and direction of the Ombudsman.

**(xi) PROTECTION OF INFORMATION VERSUS ACCESS TO
INFORMATION**

Any institution of legislative measures to protect information privacy must also take into account the public's right of access to the information.

**5.5 FREEDOM OF INFORMATION LEGISLATION :
INTERNATIONAL PERSPECTIVE**

**It behooves every man who values liberty
of conscience for himself to resist invasions
of it in the case of others**

Thomas Jefferson (in Trezza 1989 : 2)

A number of countries around the world, with a wide range of democratic political systems, have introduced freedom of information legislation and found it to be workable in practice. The best known examples are the United States of America, Sweden, Canada, and Australia. Other countries which have made some progress towards greater public access include the Netherlands, France, Norway, Denmark and Finland (Delbridge and Smith 1982 : 28).

Delbridge and Smith (1982 : 28) state that the exact formula of public access, either actual or proposed, varies considerably from country to country. It can be attributed

largely to differences between the societies and histories of the nations concerned.

Differences in the structure and form of public access according to Riley (1986 : 218) depend on the kind and extent of public pressure. In the Netherlands, for instance, it is difficult to detect any opposition to a generally worded law that lacks both a right to appeal to an independent body, and the absolute right to see the actual documentation. The United States of America has experienced the most intensive demand for freedom of information. In Sweden, public access has been a pronounced characteristic of social and political life since 1766 but within a context which differs considerably from that found in America, where pressure groups abound and there is a greater tendency to resort to the courts (Riley 1986 : 218).

Marsh (1987 : 50) states that most countries agree on the general areas of exemption from public access, namely national defence and state security; foreign relations and relations with international organizations; commercial, financial or fiscal secrets, court proceedings; prosecution and prevention of crimes; and personal or medical files, as well as other information that would constitute a breach of personal privacy.

This section will provide a brief overview of developments in countries such as the United States, Sweden, Australia and Canada. A model of freedom of information is proposed for South Africa.

Some of the issues dealt with in this chapter are common themes found in most access legislation, such as the question of independent judicial review in the event of the denial of information, time limits for responding to requests, the extent to which documents should be exempt and the documents to be covered by these exemptions.

5.5.1 UNITED STATES OF AMERICA

According to Marsh (1987 : 56) in the mid-70s, in the aftermath of Watergate and the Pentagon Papers, the United States embarked on a legislative campaign for public access to official information.

The 1966 Freedom of Information Act had led to widespread complaints of delay and obstruction. In 1974 and 1976 freedom of information had gained momentum and major administrative efforts were made to encourage its full implementation. The 1974 Privacy Act opened up an individuals' files to inspection and correction by themselves, and blocked access by anyone else (Lorch 1978 : 170).

According to the Report of the United States Privacy Council and Computer Professionals for Social Responsibility (1991 : 200) the Government in the Sunshine Act, 1976 laid certain meetings of departmental heads open to the public. The Freedom of Information Act, establishes the basic principle that public information belongs to the public.

The Report of the Privacy Protection Study Commission (1977 : 310) states that no reason need to be given for requesting information, unless it affects someone else's personal privacy, in which case a "balance of interest" principle comes into effect.

A response must be made within ten days; if it is wholly or partly negative, it must give grounds for refusal, and identify a different and more senior official to whom an appeal can be made. Appeals must be answered within 20 days; if rejected; the applicant can then take the matter to court, where it is given priority over all other business and the department must generally respond within thirty days (Report of the United States Privacy Council and Computer Professionals for Social Responsibility 1991 : 200).

According to Marsh (1987 : 58) if a case comes to court, the burden is on the particular department to justify its denial of access.

Robertson (1982 : 140) states that it is clear that an attitude of openness is crucial in making the spirit of the Freedom of Information Act work. This Act has been used by individuals, public interest and pressure groups, business corporations, journalists and scholars. For pressure groups, it has been of crucial importance, since large amounts of valuable information have been made available.

The Freedom of Information Act and the Privacy Act are intended to complement each other, providing for both public access and the proper protection of personal data (Flaherty 1989 : 335).

American freedom of information legislation has not been without its critics. Some officials have however acknowledged its value. The former Attorney General, Mr Civiletti (in Marsh 1987 : 59) said:

The Act has worked somewhat of a revolution. It has made the federal government far more open and it has exposed government wrong doing. The consequence has been that many of these wrongs have been righted. The

Act tends to make citizens better informed and provides them with the data needed for intelligent debates. In addition to these benefits, the Act undoubtedly has served to deter wrongful conduct by government officials because of fear of disclosure as a result of the commands of the Act.

5.5.2 SWEDEN

The environment in which Swedish public access system operates is altogether different. Access to information has existed according to Riley (1986 : 92) for over two centuries as a fact of life and as a constitutional principle:

The right of access to official documents is an essential part of the citizen's right to obtain and receive information and thereby one of the conditions for the free democratic moulding of opinion.

The Freedom of the Press Act gives the citizen a right of access to documents, for a fixed fee and with no legal obligation to show why the information is being sought. In the event of a denial of a document by the authorities there is an appeal to the Supreme Administrative Court. In some instances, an appeal is made to the ombudsman, an official who investigates a variety of administrative

complaints, including access to information matters (Robertson 1982 : 156).

Every department or ministry in Sweden keeps registers of incoming mail, which are immediately available to enquirers. Documents requested are either brought to the registry, or the applicant is told to which office to go. Applicants may remain anonymous (Riley 1986 : 94).

Riley (1986 : 95) states that restrictions on access to documents may be made only to safeguard what is deemed to be vital interests to the State, specifically set out in the Freedom of the Press Act. These interests (in Riley 1986 : 95) are:

- The security of the realm and its relations with other countries or international organizations;
- The state's central financial, monetary or currency policy;
- The activities of public authorities for the purpose of inspection, control or other supervision;
- The activities of public authorities for the prevention or prosecution of crime;

- The economic interests of the State or the municipalities;
- The preservation of the individual's personal and economic privacy; and
- The preservation of species of animals and plants threatened with extermination.

According to Trezza (1989 : 290) there seems to be little dissatisfaction, and few problems, with the Swedish system. Applicants may appeal to the courts against refusal of access, but such cases are not common.

5.5.3 AUSTRALIA

Australia has been moving slowly towards public access legislation since 1972. The first Freedom of Information Bill appeared in 1978, and was widely criticised as being too weak. Requests for access were to be answered within sixty days (Riley and Relyea 1983 : 18).

According to Riley (1986 : 53) the Ombudsman may investigate complaints about actions and decisions by departments in respect of requests for access to documents. Whilst the Ombudsman is able to question officials and inspect documents, he is not able to substitute a new

decision for decision of the department. He is also empowered to make recommendations to departments and ministers and, if he considers that inadequate action is taken in response to his investigations, can report to Parliament (Riley 1986 : 53).

According to Trezza (1989 : 299) freedom of information needs a supportive society and knowledgeable people who are prepared to fight for it. The Freedom of Information Act has potential to prove a very effective weapon in the conduct of government affairs. To ensure lively and informed public debate in a democratic society, it is essential that government activities be open to public scrutiny. The public must make use of the opportunities Freedom of Information rights provide in respect of government matters.

Horn and Gruber (1990 : 229) states that the more the freedom of information legislation is used, the more results it achieves, the less politicians and departments will think about destroying it.

5.5.4 CANADA

According to McCamus (1981 : 36) the turning point in the Canadian debate on freedom of information came in May 1977 with the election of the Progressive Conservatives as a

minority government. The new administration redeemed a major campaign pledge by introducing Freedom of Information Bill C-15. This Bill broadly followed the United States Model providing a general public right of access to official information subject to exemptions (McCamus 1981 : 36).

Marsh (1987 : 60) states that the Liberal Party returned to power in the ensuing federal election and soon committed itself to the re-introduction of access legislation. The new draft duly appeared in July 1980 as Bill C-43.

According to McCamus (1981 : 36) the purpose of this Act is:

To extend the present laws of Canada to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific and that decisions on the disclosure of government information should be reviewed independently of government.

Citizens are given the right of access to any record under the control of a government institution. Departments must keep registers and must respond within thirty days of any request. Non-disclosure of information must be justified by the institution keeping the records (Marsh 1987 : 60).

Marsh (1987 : 61) states that a two-tier appeal system is proposed. First to an Ombudsman type Information Commissioner and if the Commissioner recommends disclosure and the department refuses, appeal to the Courts who have power to order disclosure.

Canada is set to become the first British-style democracy to endorse the principle of a public right of access to official information (McCamus 1981 : 38).

5.6 FREEDOM OF INFORMATION LEGISLATION :

NATIONAL PERSPECTIVE

South Africa has only recently realized democracy. It is essential therefore to trace the events that transpired during the policy of separate development.

5.6.1 SOUTH AFRICA : HISTORICAL PERSPECTIVE

According to Baxter (1984 : 233) secrecy is an undoubted cause of maladministration, yet it still permeates many

facets of the administrative process. Information of real importance is withheld from the public (Baxter 1984 : 233). This was particularly true in South Africa during the apartheid system of government.

Baxter (1984 : 234) states that because of its sensitive nature, certain information ought not to be disclosed to the public. Information relating to defence, fiscal policy, international relations, or information held in confidence or of a personal nature, ought to receive protection. A completely unrestricted right of public access to the information, documents and records held by public authorities, would be unrealistic.

Kenneth Culp Davis (in Baxter 1984 : 234) states that "openness" is the natural enemy of arbitrariness and a natural ally in the fight against injustice". It is an indispensable safeguard against maladministration and corruption.

Recent South African history provides ample proof. Over the past decade a number of senior officials and cabinet ministers, protected by a plethora of laws prohibiting public access to official information, have lied to an unsuspecting public. The Information Scandal revealed corruption and the misappropriation of public funds on a massive scale, the result of the provision for secret

departmental accounts. After the abuses became known, secrecy was permitted to continue (Baxter 1984: 235).

In the case of public authorities it is claimed that secrecy is essential for effective entrepreneurial performance. However the importance of public access to information held by these institutions is just as great as in the case of ordinary departments. Access to official information is an essential safeguard against corruption (Baxter 1984 : 236).

5.6.1.1 RESTRICTIVE SOUTH AFRICAN LEGISLATION

In South Africa there were various statutes which entitled an individual to gain access to the documents and records of public authorities. In the case of business licensing authorities, persons with "reasonable grounds" may inspect all records and make copies of all documents. In the case of road transportation permits, "interested persons" and "persons affected" by application for permits may inspect and make copies of applications and related documents (Baxter 1984 : 236).

There was no general legislation providing for a right of access to such information. The general legislation that existed aimed at preventing it (Baxter 1984 : 236).

According to Baxter (1984 : 236) the most important restriction used to be the Official Secrets Act, 1956 (Act 16 of 1956). Section 3 of the Official Secrets Act contained a wide ranging prohibition against the imparting of any official information to any unauthorized person.

The Commission of Inquiry into Security Legislation recommended the replacement of the Official Secrets Act by another comprehensive piece of legislation, and this led to the Protection of Information Act, 1982 (Act 84 of 1982). This Act introduced a few limited reforms, but its broad scope did little to remove the threat to possible prosecution where information was disclosed (Baxter 1984 : 236).

5.6.2 DEVELOPMENTS IN SOUTH AFRICA

The date, 26 April 1994, signified the beginning of a new chapter when millions of South Africans went to the polls to determine their first ever democratic government. The African National Congress, with their long drawn struggle for democracy, emerged victorious (The Daily News, 8 May 1994).

One of the policies that the new government promises, is a free, democratic, transparent, and accountable government. This state of affairs can only be achieved if

there is opportunity for the citizenry to be informed about government matters. Provision is thus made in the new Constitution to inform citizens of the activities of government (The Daily News, 8 May 1994).

5.6.2.1 BILL OF FUNDAMENTAL RIGHTS AND CONSTITUTIONAL PRINCIPLES

In terms of Article 4, the Bill of Rights (1994 : 9) makes provision for a Right to Freedom of Information: *

All men and women shall be entitled to all the information necessary to enable them to make effective use of their rights as citizens or consumers.

Section 23 of the Republic of South Africa Constitution Bill, 1993 makes provision for the principle of access to official information:

Every person shall have the right of access to all information held by the state or any of its organs at any level of government in so far as such information is required for the exercise or protection of any of his or her rights.

* **A synopsis of the Fundamental Rights and Constitutional Principles for the Republic of South Africa is provided in the appendices of this study.**

5.6.2.2 RECONSTRUCTION AND DEVELOPMENT PROGRAMME (RDP)

The Reconstruction and Development Programme (1994 : 133) is an integrated, coherent, socio-economic policy framework, which seeks to mobilise the people and the country's resources toward the final eradication of apartheid and the building of a democratic, non-racial and non-sexist future.

There is provision in the Reconstruction and Development Programme (1994 : 133) inter alia, for a democratic information programme:

Open debate and transparency in government and society are crucial elements of reconstruction and development. This requires an information policy which guarantees active exchange of information and opinion among all members of society. Without the free flow of accurate and comprehensive information, the Reconstruction and Development Programme will lack the mass input necessary for its success. The new information policy must aim at facilitating exchange of information within and among communities and between the democratic government and society as a two-way process. To ensure the free flow of information, within the broad parameters of the Bill of Rights, the Freedom of Information Act must be broadened.

5.6.2.3 RECENT DEVELOPMENTS

According to a report in The Daily News (19 October 1994), Deputy President Thabo Mbeki has set up a Task Force to consult and draft a Freedom of Information Act. Mr Mbeki said that the aim "will be to give citizens access to information held by governmental institutions and other bodies exercising public power, while recognising the right to privacy on the part of citizens. The Act will also give citizens access to the proceedings of certain public bodies".

The Task Force, chaired by advocate Mojanku Gumbi, envisaged that the legislation would be handed to Parliament next year (1995). The Act would be written "in the spirit of an open and democratic society" (The Daily News, 19 October 1994).

5.6.3 PRINCIPLES FOR A FREEDOM OF INFORMATION LAW FOR SOUTH AFRICA

Riley (1986 : 91) states that for democratic government to survive and adapt to an increasingly complex and technological world, all citizens must have the power to acknowledge, both as a safeguard to fundamental rights and freedoms, and as the prerequisites to effective participation in a working democracy.

According to Amato (1994 : 151) the time has come when the rights of each citizen to have access to documents held by the various organizations of government must be established and protected by law.

Riley (1986 : 92) states that a strong and effective law must include the following features:

First: It must be a general principle of government, open to public access to information where secrecy is the exception. Where information is not released, the government must give reasons why that particular information is not released;

Second: It must provide for full and easy public access as a legal right, available to any citizen;

Third: It must list the types of documents that must be kept secret; must specify how long they are to be kept secret; must permit earlier release if this does not harm the public interest;

Fourth: It must contain provisions for the enforcement of access, by limiting the time for handling requests and appeals, requiring written reasons for a refusal and penalties for non-compliance;

Fifth: It must provide an appeal to an independent authority, including an appeal to the courts, and allow a successful applicant to recover costs;

Sixth: The scope of the law should be broad. It should allow citizens access to personal information on themselves and protection from a third party seeking information on an individual; require government departments to make available an index of the kinds of information they control; require open meetings of governmental bodies; and extend its scope to cover local government.

Seventh: The freedom of information law must override secrecy and they must be effectively amended to conform with it in practice and spirit; and

Eight: Reasons for withholding information should be set out, especially if making available that information would be likely to prejudice:

(a) the security, defence or international relations of the country;

(b) the entrusting of information to the government on a basis of confidence by:

- (i) the government of any other country or any department of such a government, or
 - (ii) any international organization or department of an international organization,
- (c) the maintenance of law or order, including the investigation and detection of offences; or
- (d) the substantial economic interests of the country.

5.6.4 BALANCING CONFLICTING INTERESTS

According to Baxter (1984 : 238) totally free access to official information is neither practical nor desirable.

Disclosure of information may jeopardise the following:

- security of the State;
- upset delicate economic policies;
- enable individuals or organisations to gain an unfair commercial advantage over competitors;
- confidences may be breached; and
- privacy may be invaded by the disclosure of sensitive or hurtful personal information (Baxter 1984 : 238).

According to Marsh (1986 : 245) the need to cater for conflicting interests is recognized in those countries which have enacted general access to information legislation.

According to Baxter (1984 : 238) the right of access to information is catered for in the following ways:

Firstly, some information must be held on record and be made permanently available for inspection on request, whilst other information must be made available within a specified time after receipt of a reasonable description of what is required;

Secondly, information is not always generally available to the public. Sometimes it must only be made available to persons who have a specified and legitimate interest. This qualification assists in maintaining the balance between the right of privacy and the need to obtain information;

Thirdly, certain categories of information are either specifically exempted by the access legislation concerned, or the legislation enables public authorities to classify certain information as secret. This ensures the protection of information where secrecy is genuinely necessary in the interests of security, confidentiality or privacy.

Finally, as a safeguard to ensure that the exemptions and qualifications are not abused by public authorities, appeal to a superior public authority, the courts, and or to an ombudsman, is provided for. With such an array of techniques and safeguards available to protect the various interests involved, South Africa is joining other democracies in enacting general access to information legislation (Baxter 1984 : 239).

5.7 SUMMARY

The protection of privacy is one of the most pressing social issues in every western country. Individuals fear the loss of control over their own personal privacy as an Information Society continues to evolve. The protection of privacy is a very complex but important issue.

Legislators have responded to widespread fears about the impact of computers on personal privacy by enacting protective laws. The following countries with privacy protection were analyzed viz. Germany, Sweden, France, Canada and the United States. Legislation enacted in these countries are briefly discussed.

Germany has a co-ordinated system of implementation for the Federal and State Data Protection Acts. Each of the States and the Federal government has its own Data Protection

Commissioner, with thirty-five professional staff to assist. The primary function of the Commissioner is to ensure that the provisions of the Data Protection Act are implemented. If he discovers violations of personal privacy, he can submit a complaint to the relevant authority, thus his powers are only advisory.

Sweden was the first country to pass a National Data Protection Law with its Data Act of 1973. It required the licensing of all personal registers in both the public and private sectors. The Data Inspection Board performs a crucial role as publicist and activist for data protection in Sweden. The staff of the Data Inspection Board is overloaded with administrative work because of the large numbers of automated personal registers in the public and private sectors. Consequently the Data Inspection Board is finding it increasingly difficult to implement data protection effectively.

France introduced a Law on Informatics and Freedoms in 1976. This law makes provision for an independent authority, the National Commission on Data Processing and Freedoms. There are seventeen members who provide information and advice to the government on the functioning of personal information systems. Since some of these members function part-time, there has been limited effectiveness in the implementation of data protection.

French data protection needs to be more fully developed.

United Kingdom was slow to enact a Data Protection Bill in 1983. This Bill establishes an independent Data Protection Registrar with a staff of about thirty to register all users of automated personal information systems in the public and private sectors. The Data Registrar has to ensure that all data users comply with the standards of fair information practices in their use of personal information. Data protection legislation in the United Kingdom needs to be more carefully reviewed if it is going to preserve the privacy of its citizens.

Canada introduced the Federal Privacy Act in 1982. There is a provision for a Privacy Commissioner which deals with complaints and violations of personal privacy. The primary need in Canada is for the nine provinces to introduce data protection legislation. The Privacy Commissioner and his staff have to function competently to make the law effective.

United States of America introduced a Privacy Act in 1974, the second national law of this kind after Sweden. The Privacy Act had structural flaws which resulted in ineffective implementation. There is no single body of independent officials charged with defending the privacy rights of its citizens. This contrasts with the

authorities found in Germany, France, Sweden and Canada. In 1977 a Privacy Protection Study Commission was created to investigate the privacy needs and protection of the American people. Given the fact that America is a forerunner in technological innovations, it is necessary to review the Computer Matching Privacy Protection Act of 1988 to promote and preserve the personal privacy of its citizens.

Previous South African Law was unable to safeguard the individual against the collection of information in databanks in both the public and private sectors. In most cases the individual was not aware that his privacy was invaded.

Section 13 of the Republic of South Africa Constitution Bill, 1993 makes provision for the right of privacy. However there has been limited development in the implementation of a Privacy Act to cater for the protection of information privacy. An independent authority charged with investigating complaints about the violation of personal privacy needs to be created. This would give effect to the promotion of personal privacy in South Africa. The Ombudsman can also play a significant role in preserving privacy. Information Privacy Protection Principles must be introduced to serve as guidelines for all institutions handling personal information.

A statutory right to personal privacy is a necessary requirement in every country committed to the democratic theory. Legislation is a vital safeguard to ensure that personal privacy is not violated. Legislation in various democracies have proved this and South Africa is no exception.

By the same token, freedom of information is also a current issue. Though there has been little movement towards new information laws in all the democracies, it is evident that some form of legislation dealing with information will emerge in most countries. The reason for this is that, with the advent of the technological revolution, there is more information available to the average person ever before in history. In addition, more information is being collected on all citizens than a decade ago.

A number of countries around the world have introduced freedom of information legislation. These countries agree on the general areas of exemption from public access, viz., national defence and state security; foreign relations and relations with international organizations; commercial, financial or fiscal secrets; court proceedings; prosecution and prevention of crimes; personal or medical files and other information that would constitute a breach of personal privacy. The following countries, with freedom of information legislation were analyzed:

United States of America introduced a Freedom of Information Act in 1966. In the early 1970's freedom of information had gained momentum and major administrative efforts were made to encourage its full implementation. The Government in the Sunshine Act made provision for certain meetings of departments to be open to the public. The Freedom of Information Act establishes a basic principle that public information belongs to the public. The Freedom of Information Act and Privacy Act are intended to complement each other, providing for public access and the proper protection of personal information.

Access to information has existed in Sweden for over two centuries as a fact of life and a constitutional principle. The Freedom of the Press Act gives the citizen a right of access to documents for a fixed fee, with no legal obligation to show why the information is sought. In the event of a denial of information, there is an appeal to the Supreme Administrative Court. Sometimes an appeal is made to the Ombudsman. Restrictions on access to information may be made only to safeguard the vital interests of the State.

Australia's first Freedom of Information Bill appeared in 1978 amidst criticisms. The Ombudsman plays a key role in investigating complaints about actions and decisions by departments in respect of requests for access to

information. To ensure lively and informed public debate, it is essential that government activities are open to public scrutiny.

Canada is set to become the first British style democracy to endorse the principle of a public right of access to official information. Canada introduced the Freedom of Information Bill C-15 in 1977. The citizen has a right to have access to any record under the control of a government institution. A two-tier appeal system is proposed, first to the Information Commissioner and secondly to the Courts who have the power to order disclosure.

South Africa followed a policy of separate development from 1948 to the early 1990's. During this time, senior officials and cabinet ministers, protected by laws prohibiting public access to official information, have lied to an unsuspecting public. There was widespread corruption in the affairs of government but the uninformed public was fooled into believing there was clean administration.

When the new government came into power, there was emphasis on clean administration, accountable and transparent government. To ensure this state of affairs, provision is made in the Reconstruction and Development Programme for a democratic information programme involving open debate

and transparency in government. The new information policy is aimed at facilitating exchange of information within and among communities and between the democratic government and citizenry.

The Bill of Fundamental Rights makes provision for a Right to Freedom of Information. Access to official information is also endorsed as one of the main constitutional principles.

A Task Force has been set up by the First Deputy President, Mr Thabo Mbeki, to investigate proposals for a Freedom of Information Act. This Freedom of Information Act must serve to complement the Privacy Act, as found in the United States of America.

The Freedom of Information Act must stipulate, inter alia., a legal right to official information; the types of information that is accessible and inaccessible; the means of appeal when disclosure is prevented; highlighting the role of the Courts and the Ombudsman in investigating the withholding of information and deciding the balance between the right to personal privacy on the one hand, and society's need to know on the other.

It can be concluded that information privacy and freedom of information are two sides of the same coin. Freedom of information means the right of a citizen to have access to governmental documents while information privacy includes the right of an individual to have access to his or her personal file. The one right cannot function without the other.

Information privacy and freedom of information are new concepts in a new South Africa.

CHAPTER 6

EMPIRICAL SURVEY OF INFORMATION PRIVACY AND FREEDOM OF INFORMATION

6.1 INTRODUCTION

An empirical study was undertaken in conjunction with the literature review, in order to determine the knowledge and attitudes of senior officials in public institutions with regards to information privacy and freedom of information.

6.2 AIM OF THE STUDY

In Chapter one, the following key questions were asked:

- (i) What does the term "information" mean in the context of South African public institutions ?
- (ii) What criteria should be used to determine which information held by public institutions be confidential and which information be made freely accessible to the public.
- (iii) What principles and mechanisms should be applied to prevent inappropriate, unauthorised or illegal access to and use of personal information held by public

institutions ?

- (iv) How can the model for the protection of information privacy rights and the promotion of access to information law be integrated in a Bill of Rights in a new South African Constitution?

The above stated questions are an integral part of the research methodology to evaluate information privacy and freedom of information in South Africa.

The aim of the study is to test the attitudes of senior public officials with reference to the information privacy concept and access to official information.

In this chapter, possible answers to the above stated questions will be based on the results of the empirical survey on information privacy and freedom of information.

The questionnaire on information privacy and freedom of information was designed taking into account some of the ideas and questions used by Harris and Westin in their research : The Dimensions of Privacy - A National Opinion Research survey of Attitudes toward Privacy.*

* **A questionnaire on Information Privacy and Freedom of Information is provided in the appendices of this study.**

The investigation procedure used in the study will be discussed. The sample will first be described and an analysis will follow. The statistical tests used in this study will also be presented.

6.3 DESCRIPTION OF SAMPLE

The study was undertaken with a total sample of 180 subjects randomly selected. The only criterion used when issuing the questionnaires were that the respondent's designation was that of a senior administrative officer.

No restrictions were placed on any other variables. Of the initial sample of 180, 100 completed questionnaires were received.

Respondents from the following public institutions were drawn namely, Department of Public Works, Receiver of Revenue, Education and Culture, Police Services, Health and Social Welfare, Manpower, Agriculture, Interior and Labour.

Senior administrative officers from Durban, Ulundi, Pretoria, Gazankulu, Lebowa, Qwaqwa, Kangwane, Eastern Transvaal, Orange Free State, Cape Town, Nelspruit, Venda and Louis Trichard made up the sample which was therefore considered representative.

6.4 PROCEDURE

The administration of questionnaires took place individually either by post or in person. Participation was voluntary and the respondents were assured of confidentiality. They was also assured of anonymity.

The respondents were clearly informed about the purpose of the research. This investigation is consequently based on a sample of 100 respondents. The research instruments used will be described. The fieldwork was undertaken during the period June to September 1994, when 180 questionnaires were distributed. The questions were in English only so that respondents could comprehend easily.

6.5 RESEARCH INSTRUMENTS

The instruments used in this survey consisted of a precoded questionnaire comprising of the following five sections, together with their objectives:

SECTION A

Personal Privacy in relation to Government Institutions

To understand the situation applicable in South Africa regarding government's collection of information and need for information privacy.

SECTION B

Privacy and Computers

To explore the attitudes towards computers and the use made of them by government.

SECTION C

Privacy and the Future

To determine what the future holds for privacy in South Africa.

SECTION D

Freedom of Information

To explore the accessibility of official information in South Africa.

SECTION E

Freedom of information and Information Privacy

To find some balance in dealing with information privacy and freedom of information.

The questionnaire comprised structured questions using the Likert Scale. According to Zimbardo and Ebbeson (1969 : 125) this method measures a person's attitude score

as the sum of his individual ratings.

Bi-polar questions were included e.g. "State yes or no". Open-ended questions gave the respondents an opportunity to make broad comments on the aspects of information privacy and freedom of information. The questionnaire included option type questions, where the respondents were allowed to add a criterion or response of their own to the list provided.

6.6 STATISTICAL ANALYSIS OF THE DATA

In order to provide empirical evidence to support or refute theories which have been mentioned, statistics has been used. Statistics is "a collection of theory and methods applied for the purpose of understanding data" (Maharaj 1993 : 87).

6.6.1 CHI-SQUARE ANALYSIS

A simple technique for describing sets of relationships is the cross-tabulation. A cross-tabulation or contingency table is "a joint frequency distribution of observations on two or more sets of variables" (Maharaj 1993 : 91).

The tabulation of subgroups serves as a measure of comparison. The statistical significance of contingency

tables is tested using the chi-square. "The chi-square analysis of a contingency table is an extension of the test to compare more than two percentages". It is used when the data consists of categorical variables, that is, when data is presented in table or column form, whereby the different rows and columns frequently represent categorical variables.

According to Maharaj (1993 : 91) in the chi-square test, "a hypothesized population distribution is compared with a distribution generated by a sample". The objective of chi-square analysis "is to determine if the differences observed in two sets of data can be attributed to sampling variation".

6.6.2 CUMULATIVE INDICES

Cumulative proportions are computed by dividing cumulative frequencies by N . Cumulative percentages are determined by multiplying cumulative proportions by 100 (Huysamen 1980 : 29).

6.7 INTERPRETATION OF RESEARCH FINDINGS

An analysis of the results of the research project will now be presented.

6.7.1 INFORMATION PRIVACY

Information is the new man-made raw material upon which all societies in future will live (Flaherty 1979 : 19). Access to information is access to power. The compilation and use of personal information are an integral part of the machinery of administration. Bureaucracies could not function without them.

According to Kreimer (1991 : 9) over the years, the government has taken on an increasing number of functions which are carried out on behalf of the citizen. In some cases, it is the citizen who has asked for the functions to be performed; in other cases the functions have been more or less imposed. Medical care, public housing, education, administration of justice, policing and environment health are just a few of the tasks carried out by government. To render these services, personal information about the citizen is necessary in order to facilitate decision-making.

Some authorities provide a long-term service and there is a need for the records to be cumulative. Apart from this exception, there is no need for authorities to retain personal details after the service has been completed, and there is no need for the details to remain confidential from the subject (Kreimer 1991 : 10).

According to Cohen (1982 : 27) just as a parent does not believe that a child should know everything, so the bureaucracy believes that the citizen should be protected from too much knowledge and that there are many things he need not know.

Citizens are being protected from knowing that unfounded allegations and unsubstantiated opinions are part of their confidential files, they are being protected from knowing that their names have been mixed up with other peoples', and as a result, that their records are highly inaccurate; they are being protected from knowing that information furnished for one purpose has been used for another, information shared with other government departments without their consent, and they are protected from knowing what type of safeguards exist to prevent the misuse of their personal information. Above all, the citizen has been prevented from knowing that his personal privacy has been violated. This has become a widespread feature of modern society (Cohen 1982 : 28).

An investigation into the term "information" in the context of South African public institutions revealed common responses. These include, inter alia., the following:

- a mutual relationship, where there is an exchange of ideas, details and knowledge between citizens and

government so that the government knows certain details about the citizens and the citizen knows certain details about the government. One entity cannot function without the other;

- in order to provide a service to the community, it is necessary to know a person's health, educational, criminal records etc, so that the public functionary can assess his background; and
- "information" refers all to kinds of personal details about an individual so that the public institution would be in a better position to render a service to him.

From the above comments it is clear that information plays a significant role in public institutions. It is a two-way exchange necessary for the administration of government and the promotion of community welfare.

"Privacy" is a concept encompassing the following ideas: that which cannot be revealed or shared with others; personal, secret, anonymity, confidentiality, not accessible to others; keeping away information from public knowledge, and the withholding of information.

In this study an analysis was undertaken to determine whether governments are the major threat to information

privacy.

Data was presented on a 2 x 2 contingency table to investigate whether subjects believed that government institutions ask for information that is unnecessarily personal and sensitive, and whether they are threats to information privacy.

TABLE 6.1

COLLECTION OF PERSONAL AND SENSITIVE INFORMATION

PERSONAL AND SENSITIVE INFORMATION	THREAT TO INFORMATION		PRIVACY
	YES	NO	
YES	50	8	58
NO	9	33	42
TOTAL	59	41	100

The majority of the subjects (50%) felt that governments do ask for information that is unnecessarily personal and sensitive and therefore constitute a threat to information privacy. However 33% of the subjects indicated otherwise. A chi-square analysis was also undertaken to investigate the relationship between government's request for personal

information and the stance with regard to information privacy.

HYPOTHESIS 1

There is a significant relationship between government's threat to information privacy and the information privacy protection principles.

CHI-SQUARE : TABLE 6.2

VARIABLE	χ^2	p
Personal and sensitive information	45.1890	0.0000
Personal information used for means other than for what it was collected	12.2345	0.0005
Personal information used without the consent of the individual	8.1893	0.0042
Personal information shared with other government departments	3.7097	0.0541*
Attempts made to keep personal information confidential	3.5298	0.1712*

* p > 0.05

The results indicate that there is a significant relationship between government threat to information privacy and the request for too personal and sensitive information, and personal information used for means other than for what it was collected. However subjects were of the opinion that the sharing of information with other government departments and attempts made to keep personal information confidential, do not contribute to government's being a threat to information privacy.

HYPOTHESIS 2

There is a significant relationship between the use of personal information for means other than for what it was collected and information being used without the consent of the individual.

CHI-SQUARE : TABLE 6.3

VARIABLE	x^2	p
Use of personal information without the individual's consent	28.9602	0.0000

The results indicate that there is a significant relationship between the use of personal information for means other than for what it was collected and information being used without the consent of the individual.

HYPOTHESIS 3

There is a significant relationship between the sharing of personal information with other government departments and attempts to keep personal information confidential.

CHI-SQUARE : TABLE 6.4

VARIABLE	χ^2	p
attempts to keep personal information confidential	1.6196	0.4449*

* p > 0.05

The analysis indicates that there is no significant relationship between the sharing of personal information with other government departments and attempts to keep personal information confidential. This means that subjects are of the opinion that sharing of information with other government departments does not infringe on

confidentiality of information.

Out of 100 respondents, 63% agreed that there should be limitations on the governments collection of personal information, while 54% agreed that the public is worried about how the government will use such information. The majority (45%) of respondents disagreed that there are adequate safeguards to prevent the misuse of information.

Various reasons have been outlined in the research, for the demands for personal information by modern societies.

These include, inter alia., the following:

- the need to become more service-orientated;
- to provide protection, safety and security for the citizen;
- modern societies are becoming more complex and people's demands necessitate the expansion of government intervention in the supply of goods and services, which in turn demands personal information;
- the need to play a greater role in the life of the citizen, to improve his quality of life and promote his community welfare; and

- advanced technology and the need to keep records as accurately as possible;

The majority (70%) of the respondents indicated that the public is concerned about threat to privacy in South Africa, while 14% were not concerned and 16% were not sure. These results are illustrated in Figure 6.1.

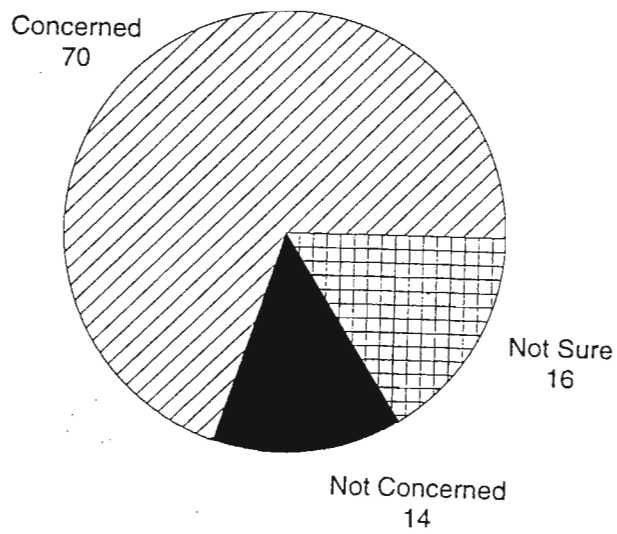
The researcher investigated whether the public in South Africa had access to correct and verify any personal information held by public institutions. Thirty eight percent (38%) of the respondents disagreed, while 41% agreed that citizens should have access to their records even if it was costly for the government to provide them.

According to research undertaken by Harris and Westin (1981 : 73) the majority of the American public and leadership groups thought that people should have access to any files that the federal government had on them regardless, of the expense and the time consumed by government departments in responding to such requests.

It can be concluded that access to personal information, even if costly for the government, is a necessary safeguard in ensuring the accuracy of information held by public institutions.

FIGURE 6.1

**GRAPHIC REPRESENTATION DEPICTING THE PUBLIC'S CONCERN ABOUT
PRIVACY IN SOUTH AFRICA**



An analysis was undertaken to determine which of the records are available for access by a requester. The results were as follows:

TABLE 6.5 : INFORMATION AVAILABLE TO A REQUESTER

Medical	69%
Criminal	34%
Educational	65%
Tax	34%
Welfare	31%
Census	25%
Other	5%

Various suggestions were made as to how an individual may challenge the accuracy, relevancy, timeliness and completeness of personal information. These included, inter alia., the following:

- an individual can only correct and verify information if he has access to such information;
- whatever information a public institution has on an individual must be made known to him, so that he can have the opportunity to check his details;

- there should be adequate facilities to continuously update one's data e.g. through computers or registers;
- certain public functionaries should be employed to check the correctness and timeliness of personal information;
- an authority should be created to continuously update personal information; and
- every six months, the public institution should send a copy of personal information to the person concerned, so that he may make corrections and changes to his file. Many respondents accepted that this was a costly exercise.

The majority (86%) of the respondents indicated that the government is the major institution responsible for protecting the privacy of individuals in South Africa. The results are depicted in Table 6.6 and Figure 6.2. while 64% of the respondents believed that the courts have a vital role to play in preserving privacy. The results are as follows:

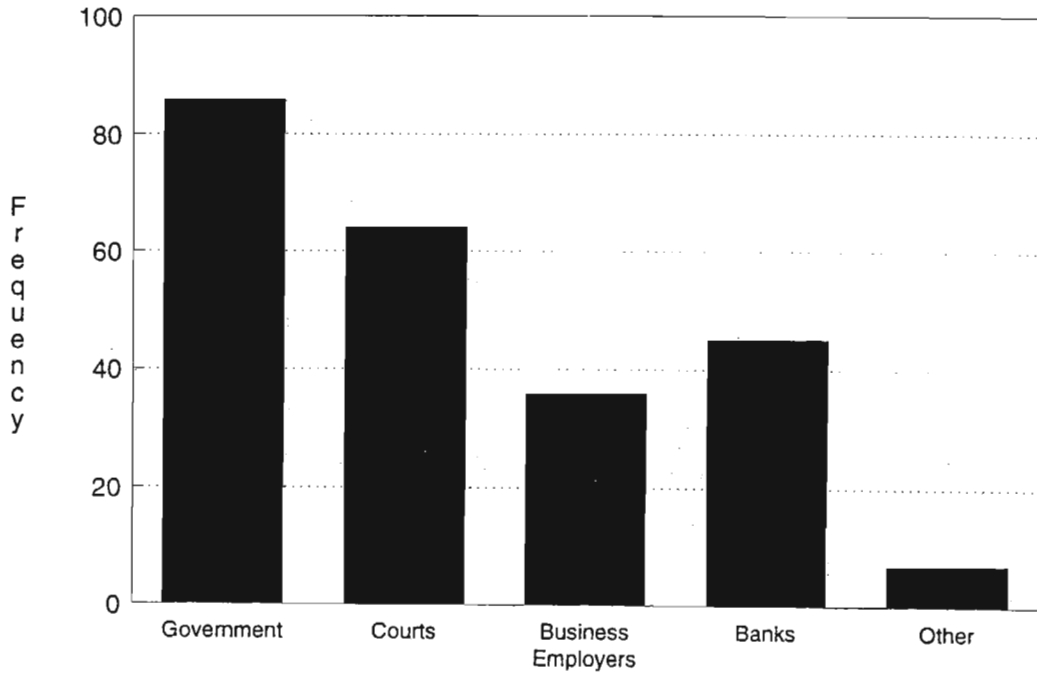
TABLE 6.6 INDIVIDUALS/INSTITUTIONS RESPONSIBLE FOR PRIVACY PROTECTION

Government	86%
Courts	64%
Business employers	36%
Banks	45%
Other	7%

According to Harris and Westin (1981 : 91) Americans appeared somewhat ambivalent in their feelings about who should be responsible for protecting their personal privacy. On the one hand, there was some evidence that they did not trust the business community, either as employers or as providers of services, to protect their personal privacy. On the other hand, there was no consensus among the public as to who should have the major responsibility for protecting the privacy of individuals. Thirty percent (30%) mentioned the Courts, 26% the Congress, and 24% state government. Because of a lack of confidence in the capacity of the courts, government or private sector, 49% of the public felt that the main responsibility for protecting the privacy of the individual should rest with the people themselves.

FIGURE 6.2

GRAPHIC REPRESENTATION ILLUSTRATING THE MAJOR INSTITUTIONS RESPONSIBLE FOR PROTECTING THE PRIVACY OF INDIVIDUALS IN SOUTH AFRICA



In sharp contrast, the public in South Africa does not have the capacity or the means to protect privacy themselves.

6.7.2 PRIVACY AND COMPUTERS

According to Bier (1980 : 20) privacy is not a vanishing value, but a value which is becoming increasingly hard to maintain. The threat to privacy originates in a social system which needs information to survive.

Rowe (1972 : 13) states that the rapid growth of technology in today's world can be viewed as an irresistible drive for efficiency, a relentless urge to achieve the maximum production of goods and services with the minimum of human effort. Computers have not only opened doors to technology never before imagined in an informational-based society, but have also brought a subtle but real challenge to the individual's right to privacy.

It must never be forgotten that computers, unlike fallible human beings, are incapable of forgetting (Cohen 1982 : 16).

The increase in the flow of information induced by the computer threatens the individual's ability to control the flow of information about himself: his privacy is thus endangered. It is storage of the "facts of his personal

life" that gives rise to the privacy fears (Rowe 1972 : 13).

An investigation into computers and its effect on privacy revealed the following results:

Forty-six percent (46%) of the respondents agreed that computers have improved the quality of life in society, while 40% agreed that South Africans believe computers threaten privacy. Fifty-six percent (56%) agreed that computers have made it easier for someone to obtain confidential personal information about individuals improperly and 35% disagreed that the use of computers should be sharply restricted in the future, while 34% disagreed that personal information in computers are adequately safeguarded.

According to research by Harris and Westin (1981 : 77) the American public acknowledged by a 60-28% majority that computers have improved the quality of life in society. The public agreed by a 64-23% majority that because computers can make use of more details about people, government can provide citizens with more individualised service. The American people were quite clear about their fears of computers as threats to personal privacy:

- by an 80-10% majority, they agreed that computers have made it easier for someone to improperly obtain confidential personal information about individuals;
- by a 52-27% majority, they disagreed that the privacy of personal information in computers is adequately safeguarded.

Sixty-three percent (63%) of the American public agreed that if privacy is to be preserved, the use of computers must be sharply restricted in the future.

Clearly, public opinion regarding the use of computers should be of concern. The message is loud and clear, if the government continues making widespread use of computers, the public must be convinced that the personal information stored in computers is adequately protected from improper use.

Forty-one percent (41%) of the respondents disagreed that South Africans can gain access to computer records and 40% disagreed that people are aware that a computerised information file on every member of the population is kept.

Forty-five percent (45%) agreed that citizens have suffered abuse because of government's computer matching programmes and 47% agreed that personal information are

kept in some data bank for purposes not known to them. Fifty-four percent (54%) agreed that the public feels threatened by having information about themselves in computers.

Fifty percent (50%) agreed that the state should have a law designed to ensure that the information on computers is kept confidential and 47% agreed that some people were prevented from getting fair treatment because of past mistakes being kept too long on computer records. Sixty-one percent (61%) believed that because computers can make use of more personal details about people, institutions can provide citizens with more individualised service than before. The majority of the respondents (58%) agreed that the computer per se is not the major threat to privacy. It is the attitude of administrators which creates the threat to personal privacy. The results are depicted in Figure 6.4.

FIGURE 6.3

**GRAPHIC REPRESENTATION DEPICTING LEGISLATION DESIGNED BY THE
STATE TO PROTECT INFORMATION PRIVACY**

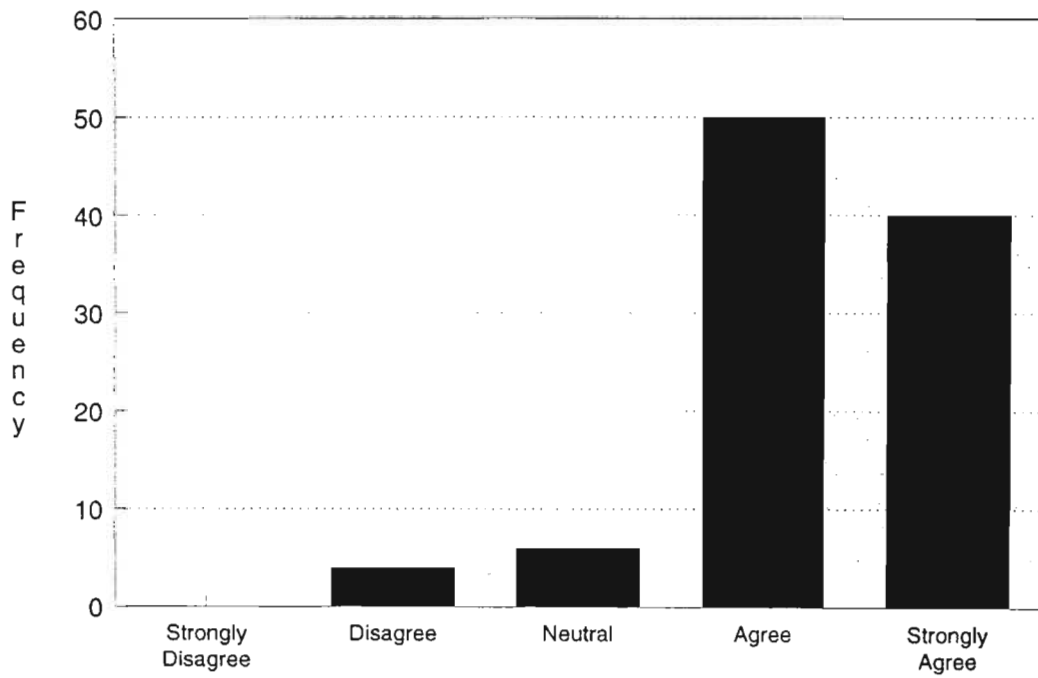
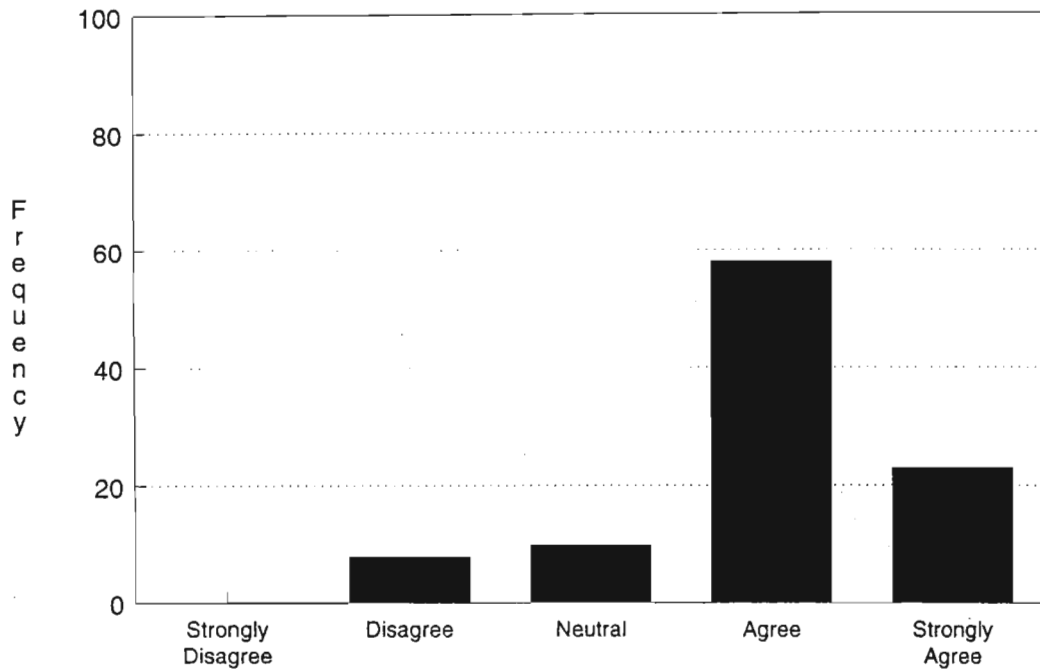


FIGURE 6.4

GRAPHIC REPRESENTATION DEPICTING THE COMPUTER AS THE MAJOR THREAT TO INFORMATION PRIVACY



6.7.3 PRIVACY AND THE FUTURE

The emergence of data protection legislation around the world is a tangible result of the growing awareness of the value of privacy. Legislation can be a marked step forward in the protection of personal privacy. Legal remedies and sanctions can assist in minimising the dangers of data banks, though it is understandable that the law may not be the only adequate solution to the problems created by the new technology (Rowe 1972 : 22).

An analysis was undertaken to investigate privacy and the future with particular reference to the protection of privacy rights.

TABLE 6.7 PRIVACY PROTECTION BY MEANS OF LEGISLATION

PRIVACY AND THE FUTURE	LEGISLATION TO	PREVENT INVASION OF PRIVACY	TOTAL
Will have lost much of their ability to keep important aspects of their lives private from the government	Laws could go a long way to help preserve privacy 52	There is nothing much that can be done to keep privacy from being eroded 30	82
Will still be able to keep privacy free from unreasonable invasions by government	11	7	18
TOTAL	63	37	100

The results indicate that 52% of the subjects felt that laws could go a long way to help preserve privacy. Despite this the same 50% maintained that in 10 years time, South African citizens will have lost much of their ability to keep important aspects of their lives private from the government. Only 7% felt that individuals will be able to protect their privacy from the government. They also maintained that there is nothing much that can be done to keep privacy from being eroded.

According to research undertaken by Harris and Westin (1981 : 83) the American public believed that they would have lost much of their ability to keep important aspects of their lives from the government in 10 years time.

HYPOTHESIS 4

In the future attempts made by government to protect the privacy of its citizens would be successful.

CHI-SQUARE : TABLE 6.8

VARIABLE	χ^2	p
Privacy and the future	0.0334	0.8549*

* p > 0.05

The results indicate that in the future attempts made by government to protect the privacy of its citizens would not be successful.

HYPOTHESIS 5

Legislation could prove to be a successful mechanism in protecting the privacy rights of citizens.

CHI-SQUARE : TABLE 6.9

VARIABLE	x²	p
Legislation to protect privacy rights	0.0406	0.8403*

p > 0.05

The results indicate that legislation may not prove to be a successful mechanism in protecting the privacy rights of citizens. The subjects therefore maintained that the government will continue to be a major threat to information privacy.

According to research undertaken by Harris and Westin (1981 : 83) the majority (67%) of the American public felt that new laws and organizational policies could go a long way to help preserve privacy.

It is apparent that the public is concerned about the potential for loss of personal privacy. The public believes they will have lost much of its privacy in relation to government. It is clear that the public is demanding that the government take effective measures to help prevent future loss of personal privacy.

HYPOTHESIS 6

The creation of a Privacy Committee is necessary to protect the privacy of individual citizens in South Africa.

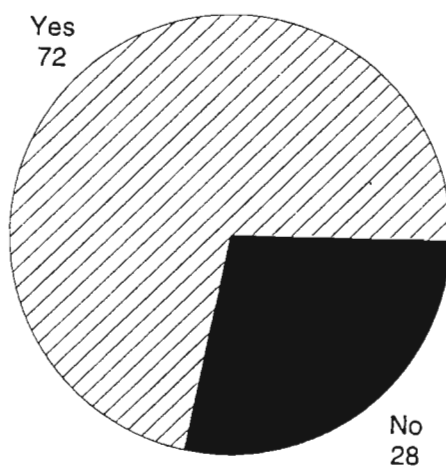
CHI-SQUARE : TABLE 6.10

VARIABLES	χ^2	p
Privacy committee to protect information privacy	6.1932	0.0128

The results indicate that the creation of Privacy Committee would contribute to the protection of privacy of South African citizens. These results are illustrated in Figure 6.5.

FIGURE 6.5

GRAPHIC REPRESENTATION DEPICTING THE NEED FOR A PRIVACY
COMMITTEE TO PROTECT PRIVACY



The researcher investigated strategies to protect the privacy of citizens in South Africa.

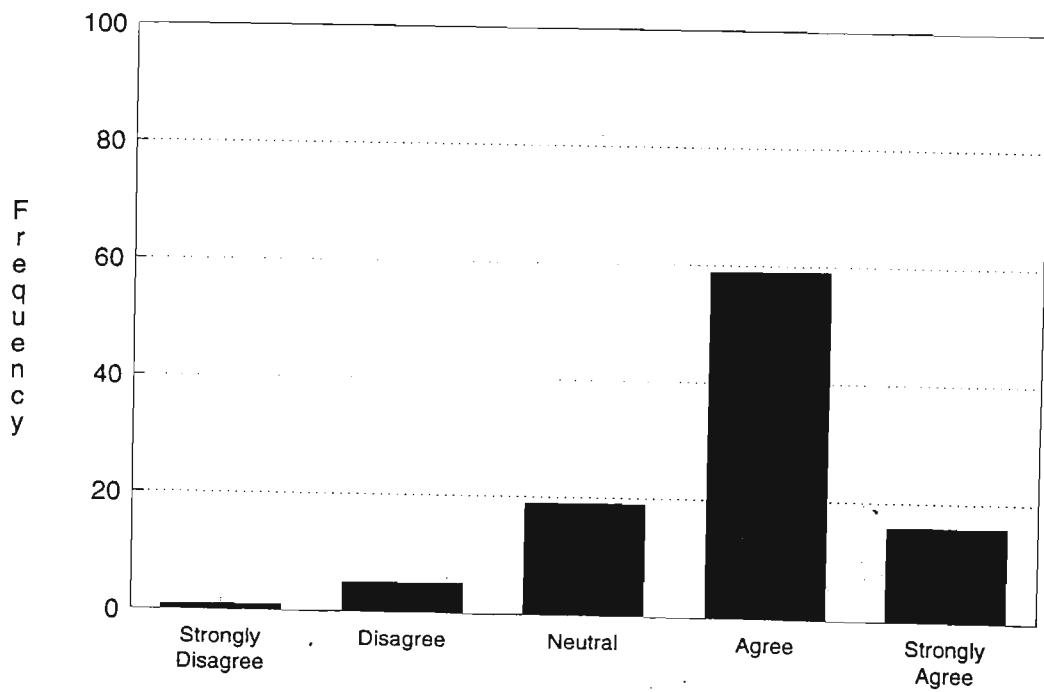
Fifty-nine percent (59%) of the respondents agreed that there should be an independent authority to handle complaints about violations of personal privacy by an institution. These results are illustrated in Figure 6.6.

According to research by Harris and Westin (1981 : 85) the American public were in sharp disagreement over the preferability of an independent body to handle complaints about violations of personal privacy by a public institutions. Sixty-two percent (62%) of the public felt that such a body was very important while leadership groups, regulatory officials and doctors felt that such a body was not at all important.

In sharp contrast, South Africans believed that legislation would not prevent the government from violating personal privacy. They strongly believed that an independent authority was important to handle complaints about violation of personal privacy.

FIGURE 6.6

**GRAPHIC REPRESENTATION DEPICTING THE NEED FOR AN INDEPENDENT
AUTHORITY TO HANDLE COMPLAINTS ABOUT VIOLATION OF PERSONAL
PRIVACY**



Fifty-four (54%) agreed that public institutions should tell individuals when information is collected on them and just how that information will be used, while 43% agreed that public institutions should obtain an individual's permission before information from his file is given out to other institutions for purposes other than why it was collected.

According to research undertaken by Harris and Westin (1981 : 88) 74% of the American public believed that it was important that public institutions provide a separate written explanation of why each piece of information was needed for anyone who asked for it. Ninety-one percent (91%) felt that an institution should obtain an individual's permission before information from his file is given out to other institutions for purposes other than for what it was collected.

Forty-seven percent (47%) agreed that public institutions should give individuals a chance to see and verify what is in their personal record. According to Harris and Westin (1981 : 90) 85% of the American public felt it was very important that institutions give individuals a chance to see and verify what is in their personal records.

It is noted that the public wants to play an active role with government in terms of reviewing their files and

giving permission before such information is released.

The majority of respondents (48 %) agreed that the state should create policies or laws to define privacy rights and 55 % agreed that comprehensive and detailed legislation is needed to protect privacy in the institutions that use personal information extensively.

6.7.4 FREEDOM OF INFORMATION

According to Hendricks et. al (1990 : 158) throughout history those who wielded power have possessed the information, and the possession of power in turn has depended to a large extent on control of the means of communication. Just as the growth of democracy has brought about the diffusion of power, so it has also brought about the diffusion of information, without which formal power is meaningless, and democracy empty.

Robertson (1982 : 56) states that any study of freedom of information must necessarily include some consideration of the political and other power structures that operate within society. The degree to which freedom of information is absent or present in a society to a large extent determines its character.

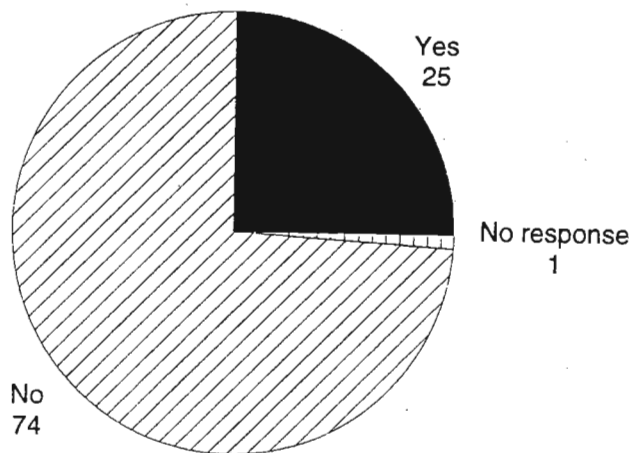
A free society must foster a high degree of freedom of information or it is a mockery. What, for example, do all the fine words about freedom and democracy ringing out from many a modern constitution mean, unless they are accompanied by that freedom to inform, and to be informed, which alone enables men and women to discuss issues and ideas on the basis of knowledge rather than ignorance, facts rather than propaganda (Hendricks et. al 1990 : 158).

Unfortunately, the results obtained in the section on freedom of information and secrecy cannot be compared or contrasted with other research as no known surveys have been conducted in these fields.

An analysis was undertaken in order to determine whether government should be allowed to function in secrecy. The majority of the subjects (74%) felt that government should not be allowed to function in secrecy. These results are presented in Figure 6.7. They simultaneously maintained that there is no conflict between accountability of government and the common need of government to perform special functions in secret.

FIGURE 6.7

GRAPHIC REPRESENTATION DEPICTING GOVERNMENT FUNCTIONING IN
SECRECY



HYPOTHESIS 7

The functioning of government in secrecy is a further threat to information privacy.

CHI-SQUARE : TABLE 6.11

VARIABLE	χ^2	p
Functioning of government in secrecy	5.1299	0.0769*

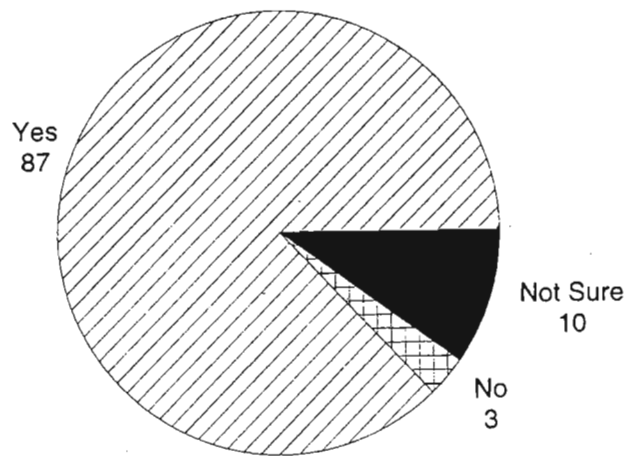
* $p > 0.05$

The results indicate that government functioning in secrecy is not a threat to information privacy.

An analysis was undertaken to determine whether a more open system of government was needed in the future. The majority of the respondents (87%) believed an open system of government was necessary, while 3% did not believe so and 10% were not sure. These results are depicted in Figure 6.8.

FIGURE 6.8

GRAPHIC REPRESENTATION DEPICTING A NEED FOR AN OPEN SYSTEM
OF GOVERNMENT



HYPOTHESIS 8

The right of official information to the public will prevent the government from functioning in secrecy.

CHI-SQUARE : TABLE 6.12

VARIABLE	x^2	p
Right to official information	11.4913	0.0216

The results indicate that one strategy to prevent the government from functioning in secrecy is to provide the public with official information.

HYPOTHESIS 9

The Freedom of Information Act would prevent the government from operating in secrecy.

CHI-SQUARE : TABLE 6.13

VARIABLE	x^2	p
Freedom of Information Act	8.0957	0.0881*

* $p > 0.05$

The results indicate that subjects are of the opinion that a Freedom of Information Act does not prevent the government from functioning in secrecy.

Forty-eight percent (48%) of the subjects agreed that citizens should have the legal right to investigate and examine the conduct of government through official information, while 61% agreed that a government that professes to be democratic ought to permit its people freedom of information. Fifty-two percent (52%) agreed there is a feeling among citizens that they are being misled and thus there is excessive pressure on the government for official information.

The majority of the respondents (61%) agreed that it becomes necessary for public institutions in some instances to disclose some information for public interest.

There were diverse comments on why the government should be allowed to keep certain information confidential:

- to protect the interests of innocent citizens;
- for the interests of national security;
- to keep law and order;

- certain information, if known, may jeopardise projects, diplomatic ties, negotiations, and governmental activities, especially if these issues are still in the pipeline;
- some information may be harmful and injurious to the public, and if known it may be detrimental to public interest; citizens may know too much for their own good; and
- to prevent panic, fear, or anxiety amongst citizens.

An analysis was undertaken to determine in what areas the government should allow access to information. The results were as follows:

TABLE 6.14 ACCESS TO INFORMATION

Financial	79%
Economic	71%
Social	64%
Political	54%
Legal	50%
Other	5%

An analysis was undertaken to determine in what areas the government should not allow access to information. The results were as follows:

TABLE 6.15 WITHHOLDING OF CERTAIN INFORMATION BY GOVERNMENT

Troop deployment, codes, plans during war	84%
Trade secrets	49%
Defence and security	69%
Law enforcement	36%
Scientific advancement	30%
Other	1%

Responses were poor on the criteria to be used to determine which information held by public institutions should be confidential and which information be made accessible. Some of the responses are outlined below:

- There is no clear-cut answer to this question. However there will only be agreement on the criteria if there is consultation amongst the various roleplayers, viz., the public, different political parties, interest and

pressure groups, technocrats from different fields of study and government.

- The extent to which the taxpayer finances the collection of information should be the determining criteria;
- The nature of the information and the purpose for which it is necessary, should be the guiding factor;
- The interests of the individual should be weighed against the interests of society;
- This is no easy task; experts from all walks of life should decide on the confidentiality of the information; confidentiality is a relative term since what is confidential to one person may not be so to others.
- Information must be divided into categories viz., high sensitivity (only for governmental knowledge); moderate sensitivity (for public knowledge); and low sensitivity (for public knowledge).
- Since "sensitivity" is also a relative term, a commission of enquiry should be appointed to investigate which information South Africans consider sensitive. In this way there will be a clear demarcation of what is for public knowledge and what is only for governmental use.

- Information should be classified into three categories:
personal
accessible
exempted.

- Lawyers for human rights and legal experts, in consultation with the public, must decide on the nature of the information in each category.

- The courts should play a meaningful role in determining the criteria to be used; and

- Public opinion surveys should be administered to decide on the categories of information which citizens want access to, and those which should be reserved for governmental purposes.

Fifty-nine percent (59%) of the respondents agreed that national security demands at times the restriction of freedom of information in order to protect the existence of the state and the framework of society. Thirty-one (31%) percent of the respondents disagreed that the government should have a right to prosecute anyone who divulges official information.

The researcher investigated what systems need to be in place to control and monitor access, to protect privacy and

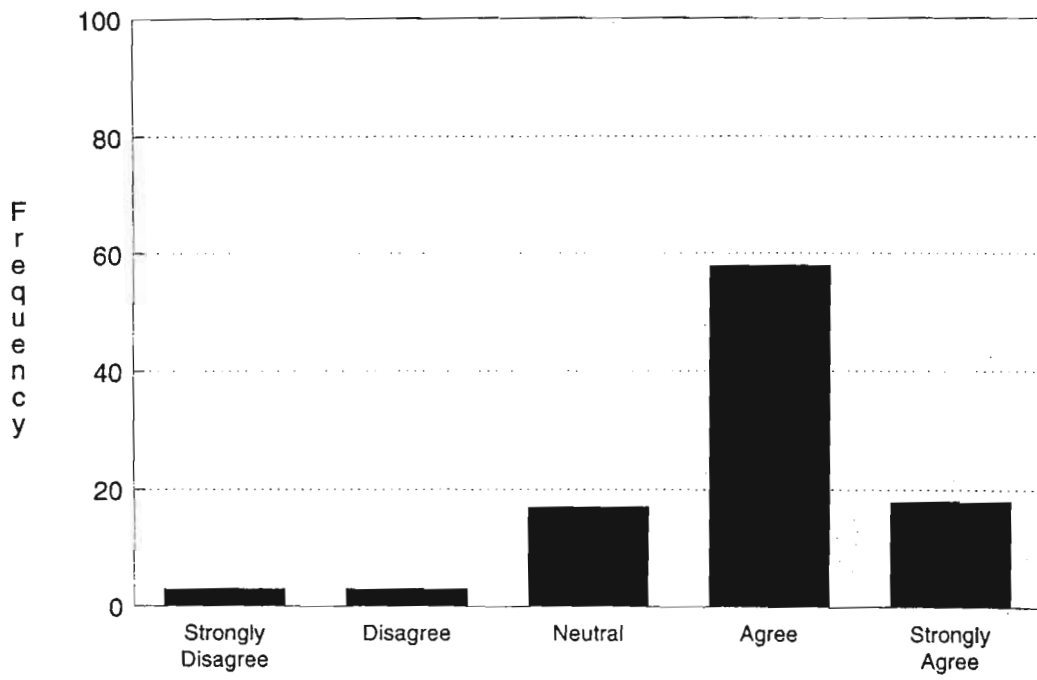
to ensure the accuracy of the information. This part of the questionnaire was poorly answered. However the following suggestions were put forward:

- It is necessary to install special codes in the computer systems, so that the person concerned will be the only one who knows his secret code. There should be protection by law for those who discover their privacy has been infringed upon;
- There should be independent privacy committees which ensure the accuracy of information and monitoring of access;
- One important safeguard is to introduce legislation that provides for the appointment of functionaries who will undertake this special function;
- There should be certain principles and guidelines to direct the procedure when information is accessible to the people; and

The majority of the respondents (58%) agreed the courts should play a role in determining when a matter is for public or government knowledge. These results are depicted in Figure 6.9.

FIGURE 6.9

GRAPHIC REPRESENTATION DEPICTING THE ROLE OF THE COURTS IN DETERMINING ACCESS TO INFORMATION



6.7.5 FREEDOM OF INFORMATION AND INFORMATION PRIVACY

The modern problem of privacy consists of achieving an appropriate balance between the genuine right to individual privacy, on the one hand, and the equally legitimate need of society to know, on the other. Here is a genuine tension, which has surely existed in earlier times, but which has become enormously aggravated by the advances of a technological society. It is because one recognises both the individual's right to privacy and society's right to know, that there is a conflict of rights (Bier 1980 : xi). The need to find an appropriate balance between protecting the confidentiality of personal information and providing access to government information is one of the common problems of advanced industrial societies (Flaherty 1979 : 19).

An analysis was undertaken to determine a balance between the need to protect information privacy on the one hand, and to allow freedom of official information on the other. Responses to this section of the questionnaire were minimal. The primary reason advanced for the lack of response is that information privacy and freedom of information are fairly new concepts in South African Public Administration.

The following answers were provided :

- There is no clear demarcation between these issues and it is difficult to find a balance. It depends on the type of government that exists. Authoritarian and autocratic governments will not allow access to official information or even access to one's personal file;
- This balance can only be found in free, democratic and open societies where the people and the government decide together on the accessibility and withholding of information;
- When the citizen allows the government to find the balance, the government always justifies official secrets and classifies all information as "confidential";
- Information that affects public interest should be accessible and certain information necessary for the administration of the state should not be made known: this is the balance.
- The interests of the public should be weighed against that of the community;
- There must be legislation allowing the accessibility of certain kinds of information and the withholding of other

kinds of information;

- Public opinion is an important indicator; and
- A commission of enquiry, comprising lawyers and human rights advocates, should investigate the balance.

Most of the respondents supported the provisions for the right to information privacy and freedom of information to be integrated in the Bill of Rights. It was felt that these provisions be drafted by policymakers in conjunction with the public, legal experts, the courts, human rights activists and academics.

The individual's claim to privacy conflicts with society's need to know. Every individual wishes to keep some aspects of his life private and this right should be respected by society.

More often than not, society wants to be privy to information that is private. A balance in this respect is difficult to maintain.

6.8 SUMMARY

In this chapter the empirical survey on information privacy and freedom of information was described and the results

interpreted against the background of the questions raised in chapter 1.

A summary of the research report is contained in the form of an article in Chapter seven.

CHAPTER 7

GENERAL CONCLUSIONS AND RECOMMENDATIONS

7.1 INTRODUCTION

In the preceding chapters a theoretical basis for information privacy and freedom of information was researched.

In this chapter certain conclusions of the study will be drawn, and certain recommendations will be made.

A definition of information privacy and freedom of information were proposed in Chapter one. This gave effect to the context in which information privacy and freedom of information were discussed throughout the course of this study.

Chapter two focused on the dynamics of information privacy. The role of the government as a major threat to information privacy was discussed.

In chapter three the increasing use of computers in government and its impact on personal privacy was researched. Information Privacy Protection Principles were analyzed as a means for preventing the abuse of personal

privacy.

Chapter four provided an insight into the concept of freedom of information as a fundamental human right against the need for government secrecy.

Chapter five analyzed the trends in information privacy protection and promotion of freedom of information legislation. An effort was made to reach an appropriate comprehension of personal privacy and freedom of information legislation for South Africa.

In Chapter six the attitudes of senior administrative officials with reference to information privacy and freedom of information were measured by using a structured questionnaire and various statistical analyses.

The conclusions drawn from the empirical survey are summarily listed below:

- (i) There is a significant relationship between government's threat to information privacy and the request for too personal and sensitive information than is necessary and personal information used for purposes other than for what it was collected.

- (ii) The results indicate that there is a significant relationship between the use of personal information for means other than for what it was collected and information being used without the consent of the individual.
- (iii) There is no significant relationship between the sharing of personal information with other government departments and attempts to keep personal information confidential.
- (iv) The subjects felt that laws could go a long way to help preserve privacy but maintained in 10 years time, South African citizens will have lost much of their ability to keep important aspects of their lives private from government.
- (v) It was found that legislation may not prove to be a successful mechanism in protecting the privacy rights of citizens. The subjects maintained the government will continue to be a major threat to information privacy.
- (vi) The creation of a Privacy Committee would contribute to the protection of privacy of South African citizens.

- (vii) Government should not be allowed to function in secrecy. Simultaneously the same respondents maintained that there is no conflict between accountability of government and the common need of government to perform special functions in secret.
- (viii) The results indicate that government functioning in secrecy is not a threat to information privacy.
- (ix) The results indicate that one strategy to prevent the government from functioning in secrecy is to provide the public with official information.
- (x) A Freedom of Information Act does not prevent the government from functioning in secrecy.

This research has culminated in a number of recommendations.

7.2 RECOMMENDATIONS

The following recommendations are made for consideration:

RECOMMENDATION ONE

FURTHER RESEARCH INTO INFORMATION PRIVACY AND FREEDOM OF INFORMATION MUST BE UNDERTAKEN

In view of the fact that this project is of a new dimension, and in view of the complexity of the subject researched, it is recommended that further research be undertaken to develop a model for information privacy and freedom of information for South Africa. It would be useful to consider the models proposed in United States of America, Federal Republic of Germany and Canada.

RECOMMENDATION TWO

A POLICY FOR INFORMATION PRIVACY AND FREEDOM OF INFORMATION SHOULD BE ADOPTED AND CONTINUALLY REVISED

This study calls for a national policy to guide the way public institutions make, use and disclose records about individuals. It looks toward a national policy that minimises intrusiveness, maximises fairness, and defines obligations with respect to the uses and disclosures that will be made of an individual's information.

There should also be a general right of access to official information, with exceptions allowed only where the government can show that information falls into one of the legally exempted categories. By introducing such legislation, South Africa would be following what is now accepted practice in many democratic countries around the world.

RECOMMENDATION THREE

INFORMATION PRIVACY PROTECTION PRINCIPLES SHOULD BE INSTITUTED BY ALL PUBLIC RECORD KEEPING AUTHORITIES

Due attention should be paid to the following information privacy protection principles:

- the principle of publicity and transparency (openness) concerning government personal information systems (no secret data banks);
- the principle of necessity and relevance governing the collection and storage of personal information;
- the principle of limiting the collection, use, storage of personal information to the maximum extent possible;
- the principle of finality (the purpose and ultimate administrative uses for personal information need to be established in advance);
- the principle of establishing and requiring responsible keepers for personal information systems;
- the principle of controlling linkages, transfers, and interconnections involving personal information;

- the principle of requiring informed consent for the collection of personal information;
- the principle of requiring accuracy and completeness in personal information systems;
- the principle of data trespass, including civil and criminal penalties for unlawful abuses of personal information;
- the requirement of special rules for protecting sensitive personal information;
- the right of access to, and corrections of, personal information systems; and
- the right to be forgotten, including the ultimate anonymization or destruction of almost all personal information.

RECOMMENDATION FOUR

AN INDEPENDENT AUTHORITY TO HANDLE COMPLAINTS ABOUT THE VIOLATIONS OF PERSONAL PRIVACY MUST BE CREATED

The public is at ease when an independent authority is created to investigate complaints about violations of

personal privacy, since independence is associated with objectivity and fairness. The public will be confident in putting forth their complaints because their cases will not be prejudiced in any way.

Such an authority can be known as a Privacy Committee headed by a Privacy Commissioner, who undoubtedly, will be a high profiled individual, with expertise in the legal field.

RECOMMENDATION FIVE

THE ROLE OF THE COURTS IN INFORMATION PRIVACY AND FREEDOM OF INFORMATION SHOULD BE HIGHLIGHTED

In South Africa, steps are being taken to make the courts more accessible and viable to the people. Clearly an independent right of appeal to the courts, either for access to personal information or official information, is an essential component for the success of information privacy and freedom of information.

RECOMMENDATION SIX

THE OMBUDSMAN IS A VITAL INSTRUMENT IN ENHANCING THE SUCCESS OF INFORMATION PRIVACY AND FREEDOM OF INFORMATION

The ombudsman should be given advisory and investigative powers. This official can investigate, inter alia., complaints alleging violations of personal privacy.

He can also investigate the reasons for the non-disclosure of certain classes of information and recommend the overturning of a decision to deny access to official information.

RECOMMENDATION SEVEN

AN EDUCATIONAL PROGRAMME SHOULD BE DESIGNED TO ACQUAINT PUBLIC ADMINISTRATORS OF THE DYNAMICS OF INFORMATION PRIVACY AND FREEDOM OF INFORMATION

Information privacy and freedom of information are new concepts in South African Public Administration. Only if these officials are equipped with the necessary knowledge, skills and attitudes will they be in a position to provide an efficient and professional service when citizens may request access to their files or access to official information.

RECOMMENDATION EIGHT

THE ADMINISTRATION OF PERSONAL INFORMATION BY PUBLIC INSTITUTIONS MUST BE EFFECTIVE

To safeguard personal information in computers, it would be wise to have computer codes so that only the individual concerned may have access to his information. In this way personal privacy is protected. Many individuals find this system acceptable because it guarantees anonymity and maintains confidentiality.

One such code could be the personal identification number (PIN) of the individual concerned. In most cases, only the individual concerned know his personal identification number.

RECOMMENDATION NINE

LEGISLATION ON INFORMATION PRIVACY AND FREEDOM OF INFORMATION SHOULD BE DRAWN UP CONCURRENTLY

Steps should be taken in due course to address information privacy and freedom of information legislation.

The proposed Privacy Act must take into account various privacy interests of the individual. These include inter alia.:

- the right to be left alone;
- the right to a private life;
- the right to control information about oneself;

- the right to limit accessibility;
- the right to minimize intrusiveness;
- the right to expect confidentiality;
- the right to secrecy; and
- the right to correct and verify personal records.

The proposed Freedom of Information Act must take cognisance of the following features:

- the types of information that is accessible and inaccessible;
- the means of appeal and the appeal system;
- the role of the Courts and the Ombudsman with respect to access to information;
- the time and place of disclosure;
- the levy (if any) for disclosure of information; and
- the reason why such information is sought;

The Privacy Act and Freedom of Information Act must serve to complement each other, providing for public access on the one hand and the proper protection of personal information on the other.

RECOMMENDATION TEN

**THE CITIZENS OF SOUTH AFRICA SHOULD NOT ALLOW THE
GOVERNMENT TO FUNCTION IN SECRECY**

Past experiences have shown that the taxpayer was the victim of severe corruption in government. This state of affairs should not be allowed to continue. One way of preventing corruption is through an open system of government, where the individual can exercise his democratic right of access to official information. In this way, accountability is maintained at all times.

7.3 SUMMARY

This chapter viewed the dissertation as a completed project and mentioned the various aspects covered in the different chapters.

In all major research projects it is necessary that an amount of groundwork be done, in order to prepare the researcher for further investigations into the subject at hand. It has transpired, during the course of this research, that the subject under investigation, namely information privacy and freedom of information, is a contentious matter.

Due to the fact that these issues have not gained momentum during the apartheid system of government added to the difficulty in assessing the reality of the situation in South Africa.

However, as South Africa heralds towards a new era, filled with optimism and brotherhood, information privacy and freedom of information will feature prominently in keeping with democratic trends prevalent throughout the world.

In conclusion, information privacy and freedom of information needs to be more extensively researched and more fully nurtured.

BIBLIOGRAPHY

1. PUBLISHED SOURCES

1.1 BOOKS

Amato, R. 1994. **Understanding the New Constitution.** Cape Town : Juta and Co

Bayat, M. S. and Sing, D. 1994. Understanding Privacy Rights in the Information Age. **Public Administration : Concepts, Theory and Practice,** edited by M. S. Bayat and I. Meyer, Pretoria : Southern Book Publishers

Baxter, L. 1984. **Administrative Law : Legal Regulation of Administrative Action in South Africa.** Cape Town : Juta and Company

Bier, W. C. 1980. **Privacy : A Vanishing Value ?** New York : Fordham University Press

Bull, H. P. 1981. **The Federal Commissioner for Data Protection.** Bonn : Typescript

Bulmer, M. 1979. **Census, Surveys and Privacy.** London : Macmillan Press

Campbell, D. and Connor, S. 1986. **On the Record :
Surveillance, Computers and Privacy.** London : Michael
Joseph Ltd

Cohen, R. N. 1982. **Whose File is it Anyway ?** Great
Britain : Russell Press

Delbridge, R. and Smith, M. 1982. **How Official Secrecy
affects Everyday Life in Britain.** London : Burnett Books
Limited

de Villiers, B. van Vuuren, D. J. and Wiechers, M.
1992. **Human Rights : Documents that Paved the Way.**
Pretoria : Sigma Press

Flaherty, D. H. 1979. **Privacy and Government Data Banks:
An International Perspective.** London : Mansell Publishing

..... 1984. **Privacy and Data Protection. An
International Bibliography.** London : Mansell Publishing

..... 1989. **Protecting Privacy in Surveillance
Societies : The Federal Republic of Germany, Sweden,
France, Canada, and the United States.** United States of
America : University of North Carolina Press

Fried, C. 1970. **An Anatomy of Values.** Cambridge: Harvard University Press

Hamelink, C. J. 1984. **Transnational Data Flows in the Information Age.** Sweden : Chartwell-Bratt

Harris, L. and Westin, A. F. 1981. **The Dimensions of Privacy : A National Opinion Research Survey of Attitudes Towards Privacy.** New York : Garland Publishing, Inc

Harrison, T. 1988. **Access to Information in Local Government.** London : Sweet and Maxwell

Hendricks, E. Hayden, T and Novik, J.D. 1990. **Your Right to Privacy : A Basic Guide to Legal Rights in an Information Society.** United States of America : Southern Illinois University Press

Hondius, F. W. 1975. **Emerging Data Protection in Europe.** Amsterdam : North-Holland Publishing Company

Horn, Z. and Gruber, N. 1990. **The Right to Know.** California : Oakland

Huysamen, G. K. 1980. **Introductory Statistics and Research Design for the Behavioural Sciences.** Cape : National Book Printers

Jones, B. L. 1989. **Garner's Administrative Law.** London:
Butterworths

Leigh, D. 1980. **The Frontiers of Secrecy : Closed
Government in Britain.** Great Britain : Junction Books

Levine, M. H. 1980 Privacy in the Tradition of the
Western World, **Privacy : A Vanishing Value ?** edited by
W. C. Bier, New York : Fordham University Press

Lorch, R. S. 1978. **Public Administration.** United States
of America : West Publishing

Madgwick, D. and Smythe, T. 1974. **The Invasion of
Privacy.** Great Britain : Pitman Publishing

Marsh, N. 1987. **Public Access to Government - held
Information: A Comparative Symposium.** London : Stevens and
Son

Mathews, A. 1978. **The Darker Reaches of Government.** Cape
Town : Juta and Co

Martin, W. J. 1988. **The Information Society.** London :
Association for Information Management

- McCamus, J. D. 1981. **Freedom of Information : Canadian Perspectives.** Toronto : Butterworth and Co
- McClellan, G. 1976. **The Right to Privacy.** New York : H W Wilson Co
- McQuoid-Mason, D. J. 1978. **The Law of Privacy in South Africa.** Republic of South Africa : Juta and Co
- Miller, A. R. 1971. **Assault on Privacy.** Michigan : University of Michigan Press
- Pitt, D. C. and Smith, B. C. 1984. **The Computer Revolution in Public Administration : The Impact of Information Technology on Government.** Great Britain : Wheatsheaf Books Ltd
- Riley, T. 1986. **Access to Government Records : International Perspectives and Trends.** Sweden : Chartwell-Bratt
- Riley, T and Relyea, H. C. 1983. **Freedom of Information Trends in the Information Age.** London : Frank Cass and Co
- Robertson, K. G. 1982. **Public Secrets : A Study in the Development of Government Secrecy.** London : Macmillan Press Ltd

Rowat, D. C. 1979. **Administrative Secrecy in Developed Countries.** New York : Columbia University Press

Rowe. B. C. 1972. **Privacy, Computers and You.** Cheshire: National Computing Centre Limited

Rule, J., McAdam, D., Stearns, L. and Uglow, D. 1980. **The Politics of Privacy : Planning for Personal Data Systems as Powerful Technologies.** New York : Elsevier North Holland, Inc

Sieghart, P. 1976. **Privacy and Computers.** Britain : Hollen Street Press Ltd

..... 1988. **Human Rights in the United Kingdom.** London : Printer Publishers

Shillinglaw, N. and Thomas, W. 1988. **The Information Society.** Craighall : A D Donker Publishers

Sloan, I. J. 1986. **Law of Privacy Rights in a Technological Society.** United States of America : Oceana Publications Inc

Teft, S. K. 1980. **Secrecy : A Cross Cultural Perspective.** New York : Human Sciences Press

Trezza, A. F. 1989. **Effective Access to Information : Today's Challenge, Tomorrow's Opportunity.** Boston : G K Hall and Co.

Wacks, R. 1989. **Personal Information : Privacy and the Law.** Oxford : Clarendon Press

..... 1980. **The Protection of Privacy.** London: Sweet and Maxwell

Warner, M. and Stone, M. 1970. **The Data Bank Society : Organizations, Computers and Social Freedom.** London : George Allen and Unwin

Westin, A. F. 1970. **Privacy and Freedom.** New York : Antheneum

Young, J. B. 1978. **Privacy.** Chichester : John Wiley and Sons

Zimbardo, P. and Ebbeson, E. B. 1969. **Influencing Attitudes and Changing Behaviour.** Reading : Addison-Wesley

Zorkoczy, P. 1982. **Information Technology : An Introduction.** London : Pitman Publishing Ltd

1.2 PERIODICALS AND JOURNALS

Ducker, J. 1985. "Electronic Information : Impact of the Data Base", **Futures**. Volume 17

Johnson, D. G. 1984 "Mapping Ordinary Morals onto the Computer Society : A Philosophical Perspective", **Journal of Social Issues**. Volume 40 No. 3

Kreimer, S. F. 1992. "Sunlight, Secrets and Scarlet Letters", **University of Pennsylvania Law Review**. Volume 140

International and Comparative Law Quarterly, 1992, Volume 41

International Commission of Jurists, 1972. "The Legal Protection of Privacy : A Comparative Survey of Ten Countries" in **International Social Science Journal**. Volume xxiv, No. 3

Milmo, P. 1993. "The New Law of Privacy", **New Law Journal**. Volume 145

Onyshko, T. 1989. "Access to Personal Information : British and Canadian Legislative Approaches", **Manitoba Law Journal**. Volume 18

Parker, R. B. 1974. "A Definition of Privacy", **Rutgers Law Review**. Rutgers Volume 2

Sing, D. 1986. "Computer Technology and Information Privacy Interests", **Politeia**. Volume 5 No. 2

Tapper, C. 1992. "New European Directions in Data Protection", **Journal of Law and Information Science**. Volume 3

Thomas, R. 1982. "Secrecy and Freedom of Information Debates in Britain", **Government and Opposition**. Volume 17

Ruebhausen, O. M. and Brim, O. G. 1965. "Privacy and Behavioural Research". **Columbia Law Review**. Columbia Volume 5

Ware, H. W. 1979. "Private Issues in the Private Sector: A Commissioner's perspectives", **Computers and Society**. Volume 9, No. 2

1.3 Dictionaries

Collins English Dictionary and Thesaurus, 1992

1.4 Reports

Report of the National Council for Civil Liberties Evidence for the Younger Committee on Privacy, 1971

Report of the Privacy Protection Study Commission, Washington, 1977

Report of the Privacy Commissioner, Canada, 1982

Report of the New South Wales Privacy Committee, New South Wales, 1983

Report of the South African Law Commission, Pretoria, Government Printer, 1987

Report of the United States Privacy Council and Computer Professionals for Social Responsibility, 1991

1.5 NEWSPAPERS

The Daily News, 8 May 1994

The Daily News, 19 October 1994

1.6 GOVERNMENT PUBLICATION

1.6.1 ACTS OF PARLIAMENT

Republic of South Africa Constitution Bill, 1993

2. UNPUBLISHED SOURCES

2.1 DISSERTATIONS

Naidoo, L. D. 1987. **The Computer as an Aid to the Public Administrator.** Unpublished Dissertation, University of Durban Westville, Durban

Maharaj, A. A. 1993. **The Impact of Health, Safety and Environmental Issues on Job Satisfaction : An Attitudinal Analysis of Employees in the Oil Industry in the greater Durban Area.** Unpublished Dissertation, University of South Africa, Pretoria

2.2 OFFICIAL DOCUMENTS

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organisation for Economic Co-operation and Development, Paris, 1981

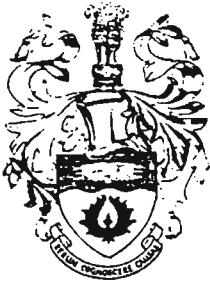
Reconstruction and Development Programme, A Policy Framework, African National Congress, 1994

A Bill of Rights for a New South Africa, 1994

2.3 SYMPOSIUMS

Freese, J. 1981. "More than Seven Years of Swedish Legislation - Analysis of Impact and Trends for the Future". **Symposium on Computer Security and Privacy.** Monte Carlo, 26 January 1981

A P P E N D I C E S



University of
Durban-Westville

PRIVATE BAG X54001 DURBAN
4000 SOUTH AFRICA
TELEGRAMS: 'UDWEST'
TELEX: 6-23228 SA
FAX: (031)820-2383
☎ (031)820-9111

DEPARTMENT OF PUBLIC ADMINISTRATION

QUESTIONNAIRE : INFORMATION PRIVACY RIGHTS OF THE INDIVIDUAL VERSUS THE PUBLIC'S
RIGHT TO FREEDOM OF INFORMATION

Dear Sir / Madam

Public concern about privacy - more specifically, the potential abuse or misuse of personal information by government - has increased steadily. This trend has stemmed largely from the increasing technological, computer-oriented nature of society in which countless determinations, ranging from hospital services, housing, social welfare grants to fire arm licences are now based on the collection of so-called "personal information".

Today, it is virtually impossible to enter a hospital or apply for any kind of financial assistance without relinquishment of some personal information.

The specific focus of this survey is to learn to what degree privacy can and should be protected in an intensely service-oriented, technological based society - a society whose collective "marketplace" is fundamentally fuelled by the collection, storage and use of the personal information of its citizens.

Another serious issue facing society today is the need to gain access to government information, simply regarded as Freedom of Information. Freedom of Information allows the citizen the opportunity to be informed about what his government is doing and why. Freedom of information would mean a substantial move to a more accountable and open system of government, a characteristic prevalent in western democracies.

This survey also examines the need for such legislation and how the citizen can best be protected against secrecy that often clouds over government. Can government maintain a proper balance between the need for personal information on its citizens in order to provide services, ensure law and order and provide for national security of the nation on the one hand, and the obligation to preserve the rights of its citizens and their personal privacy on the other ?


The aim of this questionnaire is to establish the nature and extent of the attitudes of the public officials regarding information privacy and freedom of information.

Should you have any queries or difficulty in answering the questionnaire, please contact me at the following telephone numbers:

(031) 9071855 (Work)
(031) 4000979 (Home).

Your co-operation is greatly appreciated.


P PILLAY
Masters Student


PROF. D SING
Academic Supervisor


DR M.S. BAYAT
Co-Supervisor

INSTRUCTIONS FOR THE COMPLETION OF THIS QUESTIONNAIRE

This questionnaire has been designed for computer analysis and merely requires you, the respondent, to indicate your reply by placing an "X" in the appropriate block or blocks .

Should you be of the opinion that additional comment is necessary, please use the space provided at the end of the questionnaire.

The information you provide is extremely valuable and it will be treated as confidential.

PLEASE COMPLETE THE FOLLOWING DETAILS:

NAME OF RESPONDENT:

DESIGNATION:

NAME OF INSTITUTION:

NATURE OF INSTITUTION:

**KINDLY RETURN COMPLETED QUESTIONNAIRE BEFORE
9 SEPTEMBER 1994.**

SECTION A:

PERSONAL PRIVACY IN RELATION TO GOVERNMENT INSTITUTIONS

To put a discussion of these aspects of privacy into perspective, it is necessary to understand the situation applicable in South Africa regarding government's collection of information and need for information privacy.

1. What does the term "information" mean in the context of South African public institutions?

2. What does the term "privacy" mean in the context of South African public institutions?

3. Are governments the major threat to information privacy?

Yes 01

No 02

4. Do you think government institutions ask for too personal and sensitive information than is necessary?

Yes 01

No 02

5. There should be limitations on the government's collection of personal information.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

6. When it comes to government collecting personal information, the public is worried about how they will use it.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

7. When this public institution uses information about people, there are adequate safeguards against the misuse of personal information.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

8. Has this public institution ever used personal information for means other than for what it was collected?

Yes

 01

No

 02

9. Has this public institution ever used personal information without the consent of the individual concerned?

Yes

 01

No

 02

10. Has this public institution ever shared personal information about individuals with other government departments?

Yes

 01

No

 02

11. Do you think that this public institution is currently doing enough to keep the personal information they have on individuals confidential?

Yes

 01

No

 02

12. This public institution has violated the personal privacy of an individual.

Yes

 01

No

 02

13. What is it about modern societies which encourages demands for personal information?

14. How concerned is the public about threats to their personal privacy in South Africa today?

15. Has there been any complaints from the public regarding the invasion of their personal privacy?

Yes

	01
	02

No

16. The public in South Africa has access to correct and verify any personal information held by public institutions.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

17. Citizens should have access to their records even if it is costly for the government to provide this.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

18. Has there been a public outcry to allow individuals to check their personal information?

Yes

	01
	02

No

19. Which of the following records do you feel are available for access by a requester?

- | | | |
|------------------------|--------------------------|----|
| Medical | <input type="checkbox"/> | 01 |
| Criminal | <input type="checkbox"/> | 02 |
| Educational | <input type="checkbox"/> | 03 |
| Tax | <input type="checkbox"/> | 04 |
| Welfare | <input type="checkbox"/> | 05 |
| Census | <input type="checkbox"/> | 06 |
| Other (please specify) | <input type="checkbox"/> | 07 |
-
-

20. How can a person challenge the accuracy, relevancy, timeliness and completeness of personal information?

21. Which of the following individuals/institutions should have a major responsibility for protecting the privacy of individuals in South Africa?

- | | | |
|------------------------|--------------------------|----|
| Government | <input type="checkbox"/> | 01 |
| Courts | <input type="checkbox"/> | 02 |
| Business Employers | <input type="checkbox"/> | 03 |
| Banks | <input type="checkbox"/> | 04 |
| Other (please specify) | <input type="checkbox"/> | 05 |
-
-

SECTION B:

PRIVACY AND COMPUTERS

In a very real sense, computers are at the heart of the concerns over the loss of privacy of personal information. The purpose of this section is to explore the attitudes towards computers and the use made of them by government.

1. Computers have improved the quality of life in our society.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

2. South Africans believe computers threaten privacy.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

3. Computers have made it easier for someone to obtain confidential personal information about individuals improperly.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

4. If privacy is to be preserved, the use of computers should be sharply restricted in the future.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

5. The privacy of personal information in computers are adequately safeguarded.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

6. South African citizens can gain access to computer records.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

7. People are aware that a computerised information file on every member of the population is kept.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

8. Citizens have suffered abuse because of government's computer matching programmes.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

9. Personal information about individuals are being kept in some data bank for purposes not known to them.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

10. The public does feel threatened by having information about themselves in computers.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

11. The State should have a law designed to ensure that the information on computers is kept confidential.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

12. The government now collects different kinds of information on people such as criminal records, census, military records. There is some talk of the government using computers to establish a national data bank - a computerised file which would combine all of this information in one place. Such a development is opposed by the public.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

13. Some people were prevented from getting fair treatment because of past mistakes being kept too long on computer records.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

14. Because computers can make use of more personal details about people, institutions can provide citizens with more individualised service than before.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

15. The computer per se is not the major threat to privacy. It is the attitude of administrators which creates the threat to personal privacy.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

SECTION C:

PRIVACY AND THE FUTURE

Privacy is a contemporary issue of increasing general concern. The aim of this section is to determine what the future holds for privacy in South Africa

1. When you think about life in South Africa 10 years from now, do you think the public:

a. will have lost much of their ability to keep important aspects of their lives private from the government 01

or

b. will still be able to keep their privacy free from unreasonable invasions by government 02

2. Do you think that:

a. laws could go a long way to help preserve privacy 01

or

b. there is nothing much that can be done to keep privacy from being eroded 02

3. Do you believe that a Privacy Committee should be set up if the privacy of individual citizens is to be protected in this country ?

Yes 01

No 02

4. There should be an independent authority to handle complaints about violations of personal privacy by an institution.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

05

04

03

02

01

5. Public institutions should tell individuals when information is collected on them and just how that information will be used.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

6. Public institutions should obtain an individuals permission before information from his file is given out to other institutions for purposes other than what it was collected.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

7. Public institutions should give individuals a chance to see and verify what is in their personal record.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

8. The State should create policies or laws to define privacy rights.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

9. Comprehensive and detailed legislation is needed to protect privacy in the institutions that use personal information extensively.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

SECTION D:

FREEDOM OF INFORMATION

Secrecy is an undoubted cause of maladministration, yet it still permeates many facets of the administrative process. Government secrecy has become a political issue of major proportions in recent years. The Freedom of Information issue determines the functioning of democratic government. The focus of this section is to explore the accessibility of official information in South Africa.

1. Should the government be allowed to function in secrecy?

Yes

<input type="checkbox"/>	01
<input type="checkbox"/>	02

No

2. Is there a conflict between accountability of government and the common need of government to perform certain special functions in secret?

Yes

<input type="checkbox"/>	01
<input type="checkbox"/>	02

No

3. In South Africa, the Nationalist Government was allowed to function in secrecy and this prompted a massive scale of corruption. Does this experience call for a more open system of government in future ?

4. The public has a right to official information in South Africa.

Yes

<input type="checkbox"/>	01
<input type="checkbox"/>	02

No

5. A Freedom of Information Act exist in South Africa?

Yes

<input type="checkbox"/>	01
<input type="checkbox"/>	02

No

6. Citizens should have the legal right to investigate and examine the conduct of government through official information.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

7. A government that professes to be democratic ought to permit its people freedom of information.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

8. There is a feeling among citizens that they are being misled and thus there is excessive pressure on the government for official information.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

9. Throughout the years there have been repeated stories about information marked "confidential" to prevent the public from knowing. This is justified.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

10. It becomes necessary for public institutions in some instances to disclose some information for public interest.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

11. Why should the government be allowed to keep certain information confidential?

12. In what areas do you think the government should allow access to information?

Financial	<input type="checkbox"/>	01
Economic	<input type="checkbox"/>	02
Social	<input type="checkbox"/>	03
Political	<input type="checkbox"/>	04
Legal	<input type="checkbox"/>	05
Other (please specify)	<input type="checkbox"/>	06

13. In what areas do you think the government should not allow access to information?

Troop deployment, codes, plans during war	<input type="checkbox"/>	01
Trade secrets	<input type="checkbox"/>	02
Defence and security	<input type="checkbox"/>	03
Law enforcement	<input type="checkbox"/>	04
Scientific advancement	<input type="checkbox"/>	05
Other (please specify)	<input type="checkbox"/>	06

14. What criteria should be used to determine which information held by public institutions be confidential and which information be made accessible?

15. National security demands at times the restriction of freedom of information in order to protect the existence of the State and the framework of society.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

16. The government should have a right to prosecute anyone who divulges official information.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

17. If information is available to the public, what systems need to be in place to control and monitor access, to protect privacy and to ensure the accuracy of the information?

18. The courts should play a role in determining whether a matter is for public or government knowledge.

Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
05	04	03	02	01

SECTION E:

FREEDOM OF INFORMATION AND INFORMATION PRIVACY

Freedom of information and privacy are two sides of the same coin. Freedom of information means the right of a citizen to have access to governmental documents while privacy includes the right of an individual to have access to his/her own personal file. This section aims to find some balance in dealing with information privacy and freedom of information.

1. How can the government strike a balance between the need to protect information privacy on the one hand, and allow freedom of official information on the other?

2. How can the model for information privacy rights and access to information law be integrated in a Bill of Rights in the new South African Constitution?

3. How can the individual's claim to privacy be balanced against the society's need to know?

FUNDAMENTAL RIGHTS

(As they appear in the Constitution of the
Republic of South Africa Bill, 1993)

Application

7. (1) This Chapter shall bind the legislative and executive organs of state at all levels of government.
- (2) This Chapter shall apply to all law in force and all administrative decisions taken and acts performed during the period of operation of this Constitution.
- (3) Juristic persons shall be entitled to the rights contained in this Chapter where, and to the extent that, the nature of the rights permits.
- (4) (a) When an infringement of or threat to any right entrenched in this Chapter is alleged, any person referred to in paragraph (b) shall be entitled to apply to a competent court of law for appropriate relief, which may include a declaration of rights.
- (b) The relief referred to in paragraph (a) may be sought by –
- (i) a person acting in his or her own interest;
 - (ii) an association acting in the interest of its members;
 - (iii) a person acting on behalf of another person who is not in a position to seek such relief in his or her own name;
 - (iv) a person acting as member of or in the interest of a group or class of persons; or
 - (v) a person acting in the public interest.

Equality

8. (1) Every person shall have the right to equality before the law and to equal protection of the law.
- (2) No person shall be unfairly discriminated against, directly or indirectly, and, without derogating from the generality of this provision, on one or more of the following grounds in particular: race, gender, sex, ethnic or social origin, colour, sexual orientation, age, disability, religion, conscience, belief, culture or language.
- (3) (a) This section shall not preclude measures designed to achieve adequate protection and advancement of persons or groups or categories of persons disadvantaged by unfair discrimination, in order to enable their full and equal enjoyment of all rights and freedoms.
- (b) Every person or community dispossessed of rights in land before the commencement of this Constitution under any law which would have been inconsistent with subsection (2) had that subsection been in operation at the time of the dispossession, shall be entitled to claim restitution of such rights subject to and in accordance with sections 121, 122 and 123.
- (4) *Prima facie* proof of discrimination on any of the grounds specified in subsection (2) shall be presumed to be sufficient proof of unfair discrimination as contemplated in that subsection until the contrary is established.

Life

9. Every person shall have the right to life.

Human dignity

10. Every person shall have the right to respect for and protection of his or her dignity.

Freedom and security of the person

11. (1) Every person shall have the right to freedom and security of the person, which shall include the right not to be detained without trial.
(2) No person shall be subject to torture of any kind, whether physical, mental or emotional, nor shall any person be subject to cruel, inhuman or degrading treatment or punishment.

Servitude and forced labour

12. No person shall be subject to servitude or forced labour.

Privacy

13. Every person shall have the right to his or her personal privacy, which shall include the right not to be subject to searches of his or her person, home or property, the seizure of private possessions or the violation of private communications.

Religion, belief and opinion

14. (1) Every person shall have the right to freedom of conscience, religion, thought, belief and opinion, which shall include academic freedom in institutions of higher learning.
(2) Without derogating from the generality of subsection (1), religious observances may be conducted at state or state-aided institutions under rules established by an appropriate authority for that purpose, provided that such religious observances are conducted on an equitable basis and attendance at them is free and voluntary.
(3) Nothing in this Chapter shall preclude legislation recognising –
(a) a system of personal and family law adhered to by persons professing a particular religion; and
(b) the validity of marriages concluded under a system of religious law subject to specified procedures.

Freedom of expression

15. (1) Every person shall have the right to freedom of speech and expression, which shall include freedom of the press and other media, and the freedom of artistic creativity and scientific research.
(2) All media financed by or under the control of the state shall be regulated in a manner which ensures impartiality and the expression of a diversity of opinion.

Assembly, demonstration and petition

16. Every person shall have the right to assemble and demonstrate with others peacefully and unarmed, and to present petitions.

Freedom of association

17. Every person shall have the right to freedom of association.

Freedom of movement

18. Every person shall have the right to freedom of movement anywhere within the national territory.

Residence

19. Every person shall have the right freely to choose his or her place of residence anywhere in the national territory.

Citizens' rights

20. Every citizen shall have the right to enter, remain in and leave the Republic, and no citizen shall without justification be deprived of his or her citizenship.

Political rights

21. (1) Every citizen shall have the right –
- (a) to form, to participate in the activities of and to recruit members for a political party;
 - (b) to campaign for a political party or cause; and
 - (c) freely to make political choices.
- (2) Every citizen shall have the right to vote, to do so in secret and to stand for election to public office.

Access to court

22. Every person shall have the right to have justiciable disputes settled by a court of law or, where appropriate, another independent and impartial forum.

Access to information

23. Every person shall have the right of access to all information held by the state or any of its organs at any level of government in so far as such information is required for the exercise or protection of any of his or her rights.

Administrative justice

24. Every person shall have the right to –
- (a) lawful administrative action where any of his or her rights or interests is affected or threatened;
 - (b) procedurally fair administrative action where any of his or her rights or legitimate expectations is affected or threatened;
 - (c) be furnished with reasons in writing for administrative action which affects any of his or her rights or interests unless the reasons for such action have been made public; and
 - (d) administrative action which is justifiable in relation to the reasons given for it where any of his or her rights is affected or threatened.

Detained, arrested and accused persons

25. (1) Every person who is detained, including every sentenced prisoner, shall have the right –
- (a) to be informed promptly in a language which he or she understands of the reason for his or her detention;
 - (b) to be detained under conditions consonant with human dignity, which shall include at least the provision of adequate nutrition, reading material and medical treatment at state expense;
 - (c) to consult with a legal practitioner of his or her choice, to be informed of this right promptly and, where substantial injustice would otherwise result, to be provided with the services of a legal practitioner by the state;
 - (d) to be given the opportunity to communicate with, and to be visited by, his or her spouse or partner, next-of-kin, religious counsellor and a medical practitioner of his or her choice; and
 - (e) to challenge the lawfulness of his or her detention in person before a court of law and to be released if such detention is unlawful.
- (2) Every person arrested for the alleged commission of an offence shall, in addition to the rights which he or she has as a detained person, have the right –
- (a) promptly to be informed, in a language which he or she understands, that he or she has the right to remain silent and to be warned of the consequences of making any statement;
 - (b) as soon as it is reasonably possible, but not later than 48 hours after the arrest or, if the said period of 48 hours expires outside ordinary court hours or on a day which is not a court day, the first court day after such expiry, to be brought before an ordinary court of law and to be charged or to be informed of the reason for his or her further detention, failing which he or she shall be entitled to be released;

- (c) not to be compelled to make a confession or admission which could be used in evidence against him or her; and
 - (d) to be released from detention with or without bail, unless the interests of justice require otherwise.
- (3) Every accused person shall have the right to a fair trial, which shall include the right –
- (a) to a public trial by an ordinary court of law within a reasonable time of having been charged;
 - (b) to be informed with sufficient particularity of the charge;
 - (c) to be presumed innocent and to remain silent during plea proceedings or trial and not to testify during trial;
 - (d) to adduce and challenge evidence, and not to be a compellable witness against himself or herself;
 - (e) to be represented by a legal practitioner of his or her choice or, where substantial injustice would otherwise result, to be provided with legal representation at state expense, and to be informed of these rights;
 - (f) not to be convicted of an offence in respect of any act or omission which was not an offence at the time it was committed, and not to be sentenced to a more severe punishment than that which was applicable when the offence was committed;
 - (g) not to be tried again for any offence of which he or she has previously been convicted or acquitted;
 - (h) to have recourse by way of appeal or review to a higher court than the court of first instance;
 - (i) to be tried in a language which he or she understands or, failing this, to have the proceedings interpreted to him or her; and
 - (j) to be sentenced within a reasonable time after conviction.

Economic activity

26. (1) Every person shall have the right freely to engage in economic activity and to pursue a livelihood anywhere in the national territory.
- (2) Subsection (1) shall not preclude measures designed to promote the protection or the improvement of the quality of life, economic growth, human development, social justice, basic conditions of employment, fair labour practices or equal opportunity for all, provided such measures are justifiable in an open and democratic society based on freedom and equality.

Labour relations

27. (1) Every person shall have the right to fair labour practices.
- (2) Workers shall have the right to form and join trade unions, and employers shall have the right to form and join employers' organizations.
- (3) Workers and employers shall have the right to organize and bargain collectively.
- (4) Workers shall have the right to strike for the purpose of collective bargaining.
- (5) Employers' recourse to the lock-out for the purpose of collective bargaining shall not be impaired, subject to section 33(1).

Property

28. (1) Every person shall have the right to acquire and hold rights in property and, to the extent that the nature of the rights permits, to dispose of such rights.
- (2) No deprivation of any rights in property shall be permitted otherwise than in accordance with a law.
- (3) Where any rights in property are expropriated pursuant to a law referred to in subsection (2), such expropriation shall be permissible for public purposes only and shall be subject to the payment of agreed compensation or, failing agreement, to the payment of such compensation and within such period as may be determined by a court of law as just and equitable, taking into account all relevant factors, including,

in the case of the determination of compensation, the use to which the property is being put, the history of its acquisition, its market value, the value of the investments in it by those affected and the interests of those affected.

Environment

29. Every person shall have the right to an environment which is not detrimental to his or her health or well-being.

Children

30. (1) Every child shall have the right –
- (a) to a name and nationality as from birth;
 - (b) to parental care;
 - (c) to security, basic nutrition and basic health and social services;
 - (d) not to be subject to neglect or abuse; and
 - (e) not to be subject to exploitative labour practices nor to be required or permitted to perform work which is hazardous or harmful to his or her education, health or well-being.
- (2) Every child who is in detention shall, in addition to the rights which he or she has in terms of section 25, have the right to be detained under conditions and to be treated in a manner that takes account of his or her age.
- (3) For the purpose of this section a child shall mean a person under the age of 18 years and in all matters concerning such child his or her best interest shall be paramount.

Language and culture

31. Every person shall have the right to use the language and to participate in the cultural life of his or her choice.

Education

32. Every person shall have the right –
- (a) to basic education and to equal access to educational institutions;
 - (b) to instruction in the language of his or her choice where this is reasonably practicable; and
 - (c) to establish, where practicable, educational institutions based on a common culture, language or religion, provided that there shall be no discrimination on the ground of race.

Limitation

33. (1) The rights entrenched in this Chapter may be limited by law of general application, provided that such limitation –
- (a) shall be permissible only to the extent that it is –
 - (i) reasonable; and
 - (ii) justifiable in an open and democratic society based on freedom and equality; and
 - (b) shall not negate the essential content of the right in question,
- and provided further that any limitation to –
- (aa) a right entrenched in section 10, 11, 12, 14(1), 21, 25, or 30(1)(d) or (e) or (2); or
 - (bb) a right entrenched in section 15, 16, 17, 18, 23 or 24, in so far as such right relates to free and fair political activity,

shall, in addition to being reasonable as required in paragraph (a)(i), also be necessary.

- (2) Save as provided for in subsection (1) or any other provision of this Constitution, no law, whether a rule of the common law, customary law or legislation, shall limit any right entrenched in this Chapter.

(3) The entrenchment of the rights in terms of this Chapter shall not be construed as denying the existence of any other rights or freedoms recognized or conferred by common law, customary law or legislation to the extent that they are not inconsistent with this Chapter.

(4) This Chapter shall not preclude measures designed to prohibit unfair discrimination by bodies and persons other than those bound in terms of section 7(1).

(5) (a) The provisions of a law in force at the commencement of this Constitution promoting fair employment practices, orderly and equitable collective bargaining and the regulation of industrial action shall remain of full force and effect until repealed or amended by the legislature.

(b) If a proposed enactment amending or repealing a law referred to in paragraph (a) deals with a matter in respect of which the National Manpower Commission, referred to in section 2A of the Labour Relations Act, 1956 (Act No. 28 of 1956), or any other similar body which may replace the Commission, is competent in terms of a law then in force to consider and make recommendations, such proposed enactment shall not be introduced in Parliament unless the said Commission or such other body has been given an opportunity to consider the proposed enactment and to make recommendations with regard thereto.

State of emergency and suspension

34. (1) A state of emergency shall be proclaimed prospectively under an Act of Parliament, and shall be declared only where the security of the Republic is threatened by war, invasion, general insurrection or disorder or at a time of national disaster, and if the declaration of a state of emergency is necessary to restore peace or order.

(2) The declaration of a state of emergency and any action taken, including any regulation enacted, in consequence thereof, shall be of force for a period of not more than 21 days, unless it is extended for a period of not longer than three months, or consecutive periods of not longer than three months at a time, by resolution of the National Assembly adopted by a majority of at least two-thirds of all its members.

(3) Any superior court shall be competent to enquire into the validity of a declaration of a state of emergency, any extension thereof, and any action taken, including any regulation enacted, under such declaration.

(4) The rights entrenched in this Chapter may be suspended only in consequence of the declaration of a state of emergency, and only to the extent necessary to restore peace or order.

(5) Neither any law which provides for the declaration of a state of emergency, nor any action taken, including any regulation enacted, in consequence thereof, shall permit or authorise –

(a) the creation of retrospective crimes;

(b) the indemnification of the state or of persons acting under its authority for unlawful actions during the state of emergency; or

(c) the suspension of this section, and sections 7, 8(2), 9, 10, 11(2), 12, 14, 27(1) and (2), 30(1)(d) and (e) and (2) and 33(1) and (2).

(6) Where a person is detained under a state of emergency the detention shall be subject to the following conditions:

(a) an adult family member or friend of the detainee shall be notified of the detention as soon as is reasonably possible;

(b) the names of all detainees and a reference to the measures in terms of which they are being detained shall be published in the *Gazette* within five days of their detention;

(c) when rights entrenched in sections 11 or 25 have been suspended –

(i) the detention of a detainee shall, as soon as it is reasonably possible but not later than 10 days after his or her detention, be reviewed by a court

of law, and the court shall order the release of the detainee if it is satisfied that the detention is not necessary to restore peace or order;

(ii) a detainee shall at any stage after the expiry of a period of 10 days after a review in terms of subparagraph (i) be entitled to apply to a court of law for a further review of his or her detention, and the court shall order the release of the detainee if it is satisfied that the detention is no longer necessary to restore peace or order;

(d) the detainee shall be entitled to appear before the court in person, to be represented by legal counsel, and to make representations against his or her continued detention;

(e) the detainee shall be entitled at all reasonable times to have access to a legal representative of his or her choice;

(f) the detainee shall be entitled at all times to have access to a medical practitioner of his or her choice; and

(g) the state shall for the purpose of a review referred to in paragraph (c)(i) or (ii) submit written reasons to justify the detention or further detention of the detainee to the court, and shall furnish the detainee with such reasons not later than two days before the review.

(7) If a court of law, having found the grounds for a detainee's detention unjustified, orders his or her release, such a person shall not be detained again on the same grounds unless the state shows good cause to a court of law prior to such re-detention.

Interpretation

35. (1) In interpreting the provisions of this Chapter a court of law shall promote the values which underlie an open and democratic society based on freedom and equality and shall, where applicable, have regard to public international law applicable to the protection of the rights entrenched in this Chapter, and may have regard to comparable foreign case law.

(2) No law which limits any of the rights entrenched in this Chapter, shall be constitutionally invalid solely by reason of the fact that the wording used *prima facie* exceeds the limits imposed in this Chapter, provided such a law is reasonably capable of a more restricted interpretation which does not exceed such limits, in which event such law shall be construed as having a meaning in accordance with the said more restricted interpretation.

(3) In the interpretation of any law and the application and development of the common law and customary law, a court shall have due regard to the spirit, purport and objects of this Chapter.

CONSTITUTIONAL PRINCIPLES

(As they appear in the Constitution of the Republic of South Africa Bill 1993)

I

The Constitution of South Africa shall provide for the establishment of one sovereign state, a common South African citizenship and a democratic system of government committed to achieving equality between men and women and people of all races.

II

Everyone shall enjoy all universally accepted fundamental rights, freedoms and civil liberties, which shall be provided for and protected by entrenched and justiciable provisions in the Constitution, which shall be drafted after having given due consideration to inter alia the fundamental rights contained in Chapter 3 of this Constitution.

III

The Constitution shall prohibit racial, gender and all other forms of discrimination and shall promote racial and gender equality and national unity.

IV

The Constitution shall be the supreme law of the land. It shall be binding on all organs of state at all levels of government.

V

The legal system shall ensure the equality of all before the law and an equitable legal process. Equality before the law includes laws, programmes or activities that have as their object the amelioration of the conditions of the disadvantaged, including those disadvantaged on the grounds of race, colour or gender.

VI

There shall be a separation of powers between the legislature, executive and judiciary, with appropriate checks and balances to ensure accountability, responsiveness and openness.

VII

The judiciary shall be appropriately qualified, independent and impartial and shall have the power of jurisdiction to safeguard and enforce the Constitution and all fundamental rights.

VIII

There shall be representative government embracing multi-party democracy, regular elections, universal adult suffrage, a common voters' roll, and, in general, proportional representation.

IX

Provision shall be made for freedom of information so that there can be open and accountable administration at all levels of government.

X

Formal legislative procedures shall be adhered to by legislative organs at all levels of government.

XI

The diversity of language and culture shall be acknowledged and protected, and conditions for their promotion shall be encouraged.

XII

Collective rights of self-determination in forming, joining and maintaining organs of civil society, including linguistic, cultural and religious associations, shall, on the basis of non-discrimination and free association, be recognized and protected.

XIII

The institution, status and role of traditional leadership, according to indigenous law, shall be recognized and protected in the Constitution. Indigenous law, like common law, shall be recognized and applied by the courts, subject to the fundamental rights contained in the Constitution and to legislation dealing specifically therewith.

XIV

Provision shall be made for participation of minority political parties in the legislative process in a manner consistent with democracy.

XV

Amendments to the Constitution shall require special procedures involving special majorities.

XVI

Government shall be structured at national, provincial and local levels.

XVII

At each level of government there shall be democratic representation. This principle shall not derogate from the provisions of Principle XIII.

XVIII

The powers, boundaries and functions of the national government and provincial governments shall be defined in the Constitution. Amendments to the Constitution which alter the powers, boundaries, functions or institutions of provinces shall in addition to any other procedures specified in the Constitution for constitutional amendments, require the approval of a special majority of the legislatures of the provinces, alternatively, if there is such a chamber, a two-thirds majority of a chamber of Parliament composed of provincial representatives, and if the amendment concerns specific provinces only, the approval of the legislatures of such provinces will also be needed. Provision shall be made for obtaining the views of a provincial legislature concerning all constitutional amendments regarding its powers, boundaries and functions.

XIX

The powers and functions at the national and provincial levels of government shall include exclusive and concurrent powers as well as the power to perform functions for the other levels of government on an agency or delegation basis.

XX

Each level of government shall have the appropriate and adequate legislative and executive powers and functions that will enable each level to function effectively. The allocation of powers between different levels of government shall be made on a basis which is conducive to financial viability at each level of government and to effective public administration, and which recognizes the need for and promotes national unity and legitimate provincial autonomy and acknowledges cultural diversity.

XXI

The following criteria shall be applied in the allocation of powers to the national government and the provincial governments:

1. The level at which decisions can be taken most effectively in respect of the quality and rendering of services, shall be the level responsible and accountable for the quality and

the rendering of the services, and such level shall accordingly be empowered by the Constitution to do so.

2. Where it is necessary for the maintenance of essential national standards, for the establishment of minimum standards required for the rendering of services, the maintenance of economic unity, the maintenance of national security or the prevention of unreasonable action taken by one province which is prejudicial to the interests of another province or the country as a whole, the Constitution shall empower the national government to intervene through legislation or such other steps as may be defined in the Constitution.

3. Where there is necessity for South Africa to speak with one voice, or to act as a single entity – in particular in relation to other states – powers should be allocated to the national government.

4. Where uniformity across the nation is required for a particular function, the legislative power over that function should be allocated predominantly, if not wholly, to the national government.

5. The determination of national economic policies, and the power to promote inter-provincial commerce and to protect the common market in respect of the mobility of goods, services, capital and labour, should be allocated to the national government.

6. Provincial governments shall have powers, either exclusively or concurrently with the national government, inter alia –

(a) for the purposes of provincial planning and development and the rendering of services; and

(b) in respect of aspects of government dealing with specific socio-economic and cultural needs and the general well-being of the inhabitants of the province.

7. Where mutual co-operation is essential or desirable or where it is required to guarantee equality of opportunity or access to a government service, the powers should be allocated concurrently to the national government and the provincial governments.

8. The Constitution shall specify how powers which are not specifically allocated in the Constitution to the national government or to a provincial government, shall be dealt with as necessary ancillary powers pertaining to the powers and functions allocated either to the national government or provincial governments.

XXII

The national government shall not exercise its powers (exclusive or concurrent) so as to encroach upon the geographical, functional or institutional integrity of the provinces.

XXIII

In the event of a dispute concerning the legislative powers allocated by the Constitution concurrently to the national government and provincial governments which cannot be resolved by a court on a construction of the Constitution, precedence shall be given to the legislative powers of the national government.

XXIV

A framework for local government powers, functions and structures shall be set out in the Constitution. The comprehensive powers, functions and other features of local government shall be set out in parliamentary statutes or in provincial legislation or in both.

XXV

The national government and provincial governments shall have fiscal powers and functions which will be defined in the Constitution. The framework for local government referred to in Principle XXIV shall make provision for appropriate fiscal powers and functions for different categories of local government.

XXVI

Each level of government shall have a constitutional right to an equitable share of revenue collected nationally so as to ensure that provinces and local governments are able to provide basic services and execute the functions allocated to them.

XXVII

A Financial and Fiscal Commission, in which each province shall be represented, shall recommend equitable fiscal and financial allocations to the provincial and local governments from revenue collected nationally, after taking into account the national interest, economic disparities between the provinces as well as the population and developmental needs, administrative responsibilities and other legitimate interests of each of the provinces.

XXVIII

Notwithstanding the provisions of Principle XII, the right of employers and employees to join and form employer organizations and trade unions and to engage in collective bargaining shall be recognized and protected. Provision shall be made that every person shall have the right to fair labour practises.

XXIX

The independence and impartiality of a Public Service Commission, a Reserve Bank, an Auditor-General and Public Protector shall be provided for and safeguarded by the Constitution in the interests of the maintenance of effective public finance and administration and a high standard of professional ethics in the public service.

XXX

1. There shall be an efficient, non-partisan, career-orientated public service broadly representative of the South African community, functioning on a basis of fairness and which shall serve all members of the public in an unbiased and impartial manner, and shall, in the exercise of its powers and in compliance with its duties, loyally execute the lawful policies of the government of the day in the performance of its administrative functions. The structures and functioning of the public service, as well as the terms and conditions of service of its members, shall be regulated by law.
2. Every member of the public service shall be entitled to a fair pension.

XXXI

Every member of the security forces (police, military and intelligence), and the security forces as a whole, shall be required to perform their functions and exercise their powers in the national interest and shall be prohibited from furthering or prejudicing party political interest.

XXXII

The Constitution shall provide that until 30 April 1999 the national executive shall be composed and shall function substantially in the manner provided for in Chapter 6 of this Constitution.

XXXIII

The Constitution shall provide that, unless Parliament is dissolved on account of its passing a vote of no-confidence in the Cabinet, no national election shall be held before 30 April 1999.

Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1981)

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:
 - a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;
 - b) "personal data" means any information relating to an identified or identifiable individual (data subject);
 - c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.
3. These Guidelines should not be interpreted as preventing:
 - a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;
 - b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
 - c) the application of the Guidelines only to automatic processing of personal data.

4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

- a) as few as possible, and
- b) made known to the public.

5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

PART TWO BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

Security Safeguards Principle

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

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identify and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him
 - i) within a reasonable time;
 - ii) at a charge, if any, that is not excessive;
 - iii) in a reasonable manner; and
 - iv) in a form that is readily intelligible to him;
- c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

PART THREE BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes

specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

PART FOUR NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:

- a) adopt appropriate domestic legislation;
- b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
- c) provide for reasonable means for individuals to exercise their rights;
- d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
- e) ensure that there is no unfair discrimination against data subjects.

PART FIVE INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.

21. Member countries should establish procedures to facilitate:

- i) information exchange related to these Guidelines, and
- ii) mutual assistance in the procedural and investigative matters involved.

22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

Council of Europe: Extracts from the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)

PREAMBLE

The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:

CHAPTER I — GENERAL PROVISIONS

Article 1

Object and purpose

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Article 2

Definitions

For the purposes of this convention:

a. "personal data" means any information relating to an identified or identifiable individual ("data subject");

b. "automated data file" means any set of data undergoing automatic processing;

c. "automatic processing" includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;

d. "controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.

Article 3

Scope

1. The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.

2. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:

a. that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law;

b. that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;

c. that it will also apply this convention to personal data files which are not processed automatically.

3. Any State which has extended the scope of this convention by any of the declarations provided for in sub-paragraph 2.b or c above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.

4. Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.a above may not claim the application of this convention to such categories by a Party which has not excluded them.

5. Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraphs 2.b and c above may not claim the application of this convention on these points with respect to a Party which has made such extensions.

6. The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

CHAPTER II — BASIC PRINCIPLES FOR DATA PROTECTION

Article 4

Duties of the Parties

1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

2. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

Article 5

Quality of data

Personal data undergoing automatic processing shall be:

- a. obtained and processed fairly and lawfully;
- b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
- d. accurate and, where necessary, kept up to date;
- e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 6

Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

Article 7

Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

Article 8

Additional safeguards for the data subject

Any person shall be enabled:

- a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
- b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored

in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs *b* and *c* of this article is not complied with.

Article 9

Exceptions and restrictions

1. No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

3. Restrictions on the exercise of the rights specified in Article 8, paragraphs *b*, *c* and *d*, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Article 10

Sanctions and remedies

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

Article 11

Extended protection

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data sub-

jects a wider measure of protection than that stipulated in this convention.

CHAPTER III — TRANSBORDER DATA FLOWS

Article 12

Transborder flows of personal data and domestic law

1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.
2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.
3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:
 - a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
 - b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

European Commission: Proposal for a Council Directive concerning the Protection of Individuals in relation to the Processing of Personal Data (1990)

Council of the European Communities,

having regard to the treaty establishing the European Economic Community, and in particular Articles 100a and thereof,

having regard to the proposal from the Commission,

in cooperation with the European Parliament,

having regard to the opinion of the Economic and Social Committee,

Whereas the objectives of the Community, as laid down in the treaty as amended by the Single European Act, include establishing an ever closer union among the peoples of Europe, fostering closer relations between the peoples belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitutions and laws of the member states and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

Whereas the establishment and the functioning of an internal market in which, in accordance with Article 8a of the treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely, regardless of the member states in which they are processed or requested, but also that fundamental rights should be safeguarded in view of the increasingly frequent recourse in the Community to the processing of personal data in the various spheres of economic and social activity;

Whereas the internal market comprises an area without frontiers; wherefor that reason, the national authorities in the various member states are in-

creasingly being called upon, by virtue of the operation of Community law, to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another member state;

4 Whereas the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

5 Whereas the difference in levels of protection of privacy in relation to the processing of personal data afforded in the member states may prevent the transmission of such data from the territory of one member state to that of another member state; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

6 Whereas in order to remove the obstacles to flows of personal data, the level of protection of privacy in relation to the processing of such data must be equivalent in all the member states; whereas to that end it is necessary to approximate the relevant laws;

7 Whereas the object of the national laws on the processing of personal data is to protect fundamental rights, notably the right to privacy which is recognized both in Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

8 Whereas the principles underlying the protection of privacy in relation to the processing of personal data set forth in this directive may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

9 Whereas the protection principles must apply to all data files where the activities of the controller of the file are governed by Community law; whereas public-sector files which are not governed by Community law should, as is provided for in the resolution of the representatives of the governments of the member states of the European Communities meeting within the council of . . . , be subject to the same protection principles set forth in national laws; whereas, however, data files falling exclusively within the confines of the exercise of a natural person's right to privacy, such as personal address files, must be excluded;

10 Whereas any processing of personal data in the Community should be carried out in accordance with the law of the member state in which the data file is located so that individuals are not deprived of the protection to which they are entitled under this directive; whereas, in this connection, each part of a data file divided among several member states must be considered a separate data file and transfer to a non-member country must not be a bar to such protection;

11 Whereas any processing of personal data must be lawful; whereas such lawfulness must be based on the consent of the data subject or on Community or national law;

12 Whereas national laws may, under the conditions laid down in this directive, specify rules on the lawfulness of processing; whereas, however, such a possibility cannot serve as a basis for supervision by a member state other than the state in which the data file is located, the obligation on the part of the

latter to ensure, in accordance with this directive, the protection of privacy in relation to the processing of personal data being sufficient, under Community law, to permit the free flow of data;

13 Whereas the procedures of notification, in respect of public- or private-sector data files, and provision of information at the time of first communication, in respect of private-sector data files, are designed to ensure the transparency essential to the exercise by the data subject of the right of access to data relating to him;

14 Whereas the data subject must, if his consent is to be valid and when data relating to him are collected from him, be given accurate and full information;

15 Whereas the data subject must be able to exercise the right of access in order to verify the lawfulness of the processing of data relating to him and their quality;

16 Whereas, if data are to be processed, they must fulfill certain requirements; whereas the processing of data which are capable by their very nature of infringing the right to privacy must be prohibited unless the data subject gives his explicit consent; whereas, however, on important public-interest grounds, notably in relation to the medical profession, derogations may be granted on the basis of a law laying down precisely and strictly the conditions governing and limits to the processing of this type of data;

17 Whereas the protection of privacy in relation to personal data requires that appropriate security measures be taken, both at the level of design and at that of the techniques of processing, to prevent any unauthorized processing;

18 Whereas as regards the media the member states may grant derogations from the provisions of this directive insofar as they are designed to reconcile the right to privacy with the freedom of information and the right to receive and impart information, as guaranteed, in

particular in Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms;

19 Whereas the member states must encourage the drawing up, by the business circles concerned, of European codes of conduct or professional ethics relating to certain specific sectors; whereas the commission will support such initiatives and will take them into account when it considers the appropriateness of new, specific measures in respect of certain sectors;

20 Whereas, in the event of non-compliance with this directive, liability in any action for damages must rest with the controller of the file; whereas dissuasive sanctions must be applied in order to ensure effective protection;

21 Whereas it is also necessary that the transfer of personal data should be able to take place with third countries having an adequate level of protection; whereas, in the absence of such protection in third countries, this directive provides, in particular, for negotiation procedures with those countries;

22 Whereas the principles contained in this directive give substance to and amplify those contained in the Council of Europe Convention of January 28, 1981 for the Protection of Individuals with Regard to Automatic Processing of Personal Data;

23 Whereas the existence in each member state of an independent supervisory authority is an essential component of the protection of individuals in relation to the processing of personal data; whereas at Community level a Working Party on the Protection of Personal Data must be set up and be completely independent in the performance of its functions; whereas having regard to its specific nature it must advise the commission and contribute to the uniform application of the national rules adopted pursuant to this directive;

24 Whereas the adoption of additional measures for applying the prin-

ciples set forth in this directive calls for the conferment of rule-making powers on the commission and the establishment of an Advisory Committee in accordance with the procedures laid down in Council Decision 87/373/EEC (*Official Journal* No L 197, July 18, 1987, p 33),

Has adopted this directive:

Chapter I—General Provisions

Article 1—Object of the Directive

1 The member states shall ensure, in accordance with this directive, the protection of the privacy of individuals in relation to the processing of personal data contained in data files.

2 The member states shall neither restrict nor prohibit the free flow of personal data between member states for reasons to do with the protection afforded under paragraph 1.

Article 2—Definitions

For the purposes of this directive:

(a) 'personal data' means any information relating to an identified or identifiable individual ('data subject'); an identifiable individual is notably an individual who can be identified by reference to an identification number or a similar identifying particular;

(b) 'depersonalize' means to modify personal data in such a way that the information they contain can no longer be associated with a specific individual or an individual capable of being determined except at the price of an excessive effort in terms of staff, expenditure and time;

(c) 'personal data file' (file) means any set of personal data, whether centralized or geographically dispersed, undergoing automatic processing or which, although not undergoing automatic processing, are structured and ac-

able in an organized collection according to specific criteria in such a way as to facilitate their use or combination;

(b) 'processing' means the following operations, whether or not performed by automated means: the recording, storage or combination of data, and the alteration, use or communication, including transmission, dissemination, retrieval, blocking and erasure;

(c) 'controller of the file' means the natural or legal person, public authority, agency or other body competent under Community law or the national law of a member state to decide what is the purpose of the file, which categories of personal data will be included, which operations will be applied to them and which third parties may have access to them;

(d) 'supervisory authority' means the independent public authority or other independent body designated by each member state in accordance with Article 6 of this directive;

(e) 'public sector' means all the authorities, organizations and entities of a member state that are governed by public law, with the exception of those which carry on an industrial or commercial activity, and bodies and entities governed by private law where they take part in the exercise of official authority;

(f) 'private sector' means any natural person or association, including public-sector authorities, organizations and entities insofar as they carry on an industrial or commercial activity.

Article 3—Scope

1 Each member state shall apply this directive to files in the public and private sectors with the exception of files in the public sector where the activities of that sector do not fall within the scope of Community law.

This directive shall not apply to files held by:

(a) an individual solely for private

and personal purposes; or

(b) non-profit-making bodies, notably of a political, philosophical, religious, cultural, trade-union, sporting or leisure nature, as part of their legitimate aims, on condition that they relate only to those members and corresponding members who have consented to being included therein and that they are not communicated to third parties.

Article 4—Law Applicable

1 Each member state shall apply this directive to:

(a) all files located in its territory;

(b) the controller of a file resident in its territory who uses from its territory a file located in a third country whose law does not provide an adequate level of protection, unless such use is only sporadic.

2 Each member state shall apply Articles 5, 6, 8, 9, 10, 17, 18 and 21 of this directive to a user consulting a file located in a third country from a terminal located in the territory of a member state, unless such use is only sporadic.

3 Where a file is moved temporarily from one member state to another, the latter shall place no obstacle in the way and shall not require the completion of any formalities over and above those applicable in the member state in which the file is normally located.

Chapter II—Lawfulness of Processing in the Public Sector

Article 5—Principles

1 Subject to Article 6 the member states shall, with respect to files in the public sector, provide in their law that:

(a) the creation of a file and any other processing of personal data shall be lawful insofar as they are necessary for the performance of the tasks of the public authority in control of the file;

(b) the processing of data for a purpose other than that for which the file was created shall be lawful if:

— the data subject consents thereto; or

— it is effected on the basis of Community law, or of a law, or a measure taken pursuant to a law of a member state conforming with this directive which authorizes it and defines the limits thereto; or

— the legitimate interests of the data subject do not preclude such change of purpose; or

— it is necessary in order to ward off an imminent threat to public order or a serious infringement of the rights of others.

Article 6—Processing in the Public Sector Having as Its Object the Communication of Personal Data

1 The member states shall provide in their law that the communication of personal data contained in the files of a public-sector entity shall be lawful only if:

(a) it is necessary for the performance of the tasks of the public-sector entity communicating or requesting communication of the data; or

(b) it is requested by a natural or legal person in the private sector who invokes a legitimate interest, on condition that the interest of the data subject does not prevail.

2 Without prejudice to paragraph 1, the member states may specify the conditions under which the communication of personal data is lawful.

3 The member states shall provide in their law that, in the circumstances referred to in paragraph 1(b), the controller of the file shall inform data subjects of the communication of personal data. The member states may provide for the replacing of such provision of information by prior authorization by the supervisory authority.

Article 7—Obligation to Notify the Supervisory Authority

1 The member states shall provide in their law that the creation of a public-sector file the personal data in which might be communicated shall be notified in advance to the supervisory authority and recorded in a register kept by that authority. The register shall be freely available for consultation.

2 The member states shall specify the information which must be notified to the supervisory authority. That information shall include at least the name and address of the controller of the file, the purpose of the file, a description of the types of data it contains, the third parties to whom the data might be communicated and a description of the measures taken pursuant to Article 18.

3 The member states may provide that paragraphs 1 and 2 shall apply to other public-sector files and that consultation of the register may be restricted for the reasons stated in Article 15(1).

Chapter III—Lawfulness of Processing in the Private Sector

Article 8—Principles

1 The member states shall provide in their law that, without the consent of the data subject, the recording in a file and any other processing of personal data shall be lawful only if it is effected in accordance with this directive and if:

(a) the processing is carried out under a contract, or in the context of a quasi-contractual relationship of trust, with the data subject and is necessary for its discharge; or

(b) the data come from sources generally accessible to the public and their processing is intended solely for correspondence purposes; or

(c) the controller of the file is pursuing a legitimate interest, on condition

that the interest of the data subject does not prevail.

2 The member states shall provide in their law that it shall be for the controller of the file to ensure that no communication is incompatible with the purpose of the file or is contrary to public policy. In the event of online consultation the same obligations shall be incumbent on the user.

3 Without prejudice to paragraph 1 the member states may specify the conditions under which the processing of personal data is lawful.

Article 9—Obligation to Inform the Data Subject

1 The member states shall, with respect to the private sector, provide in their law that at the time of first communication or of the affording of an opportunity for online consultation the controller of the file shall inform the data subject accordingly, indicating also the purpose of the file, the types of data stored therein and his name and address.

2 The provision of information under paragraph 1 shall not be mandatory in the circumstances referred to in Article 8(1)(b). There shall be no obligation to inform where communication is required by law.

3 If the data subject objects to communication or any other processing, the controller of the file shall cease the processing objected to unless he is authorized by law to carry it out.

Article 10—Special Exceptions to the Obligation to Inform the Data Subject

If the provision of information to the data subject provided for in Article 9(1) proves impossible or involves a disproportionate effort, or comes up against the overriding legitimate interests of the controller of the file or a similar interest of a third party, the member states may provide in their law that the supervi-

sory authority may authorize a derogation.

Article 11—Obligation to Notify the Supervisory Authority

1 The member states shall provide in their law that the controller of the file shall notify the creation of a personal data file where the data are intended to be communicated and do not come from sources generally accessible to the public. The notification shall be made to the supervisory authority of the member state in which the file is located or, if it is not located in a member state, to the supervisory authority of the member state in which the controller of the file resides. The controller of the file shall notify to the competent national authorities any change in the purpose of the file or any change in his address.

2 The member states shall specify the information which must be notified to the supervisory authority. That information shall include at least the name and address of the controller of the file, the purpose of the file, a description of the types of data it contains, the third parties to whom the data might be communicated and a description of the measures taken pursuant to Article 18.

3 The member states may provide that paragraphs 1 and 2 shall apply to other private-sector files and that the information referred to in paragraph 2 shall be accessible to the public.

Chapter IV—Rights of Data Subjects

Article 12—Informed Consent

Any giving of consent by a data subject to the processing of personal data relating to him within the meaning of this directive shall be valid only if:

(a) the data subject is supplied with the following information:

—the purposes of the file and the

types of data stored;

– the type of use and, where appropriate, the recipients of the personal data contained in the file;

– the name and address of the controller of the file;

(b) it is specific and express and specifies the types of data, forms of processing and potential recipients covered by it;

(c) it may be withdrawn by the data subject at any time without retroactive effect.

Article 13—Provision of Information at the Time of Collection

1 The member states shall guarantee individuals from whom personal data are collected the right to be informed at least about:

(a) the purposes of the file for which the information is intended; and

(b) the obligatory or voluntary nature of their reply to the questions to which answers are sought; and

(c) the consequences if they fail to reply; and

(d) the recipients of the information; and

(e) the existence of the right of access to and rectification of the data relating to them; and

(f) the name and address of the controller of the file.

2 Paragraph 1 shall not apply to the collection of information where to inform the data subject would prevent the exercise of the supervision and verification functions of a public authority or the maintenance of public order.

Article 14—Additional Rights of Data Subjects

The member states shall grant a data subject the following rights:

1 to oppose, for legitimate reasons, the processing of personal data relating to him;

2 not to be subject to an administrative or private decision involving an assessment of his conduct which has as its sole basis the automatic processing of personal data defining his profile or personality;

3 to know of the existence of a file and to know its main purposes and the identity and habitual residence, headquarters or place of business of the controller of the file;

4 to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in a file and communication to him of such data in an intelligible form; the member states may provide that the right of access to medical data may be exercised only through a doctor;

5 to obtain, as the case may be, rectification, erasure or blocking of such data if they have been processed in violation of the provisions of this directive;

6 to obtain upon request and free of charge the erasure of data relating to him held in files used for market research or advertising purposes;

7 to obtain, in the event of the application of paragraph 5 and if the data have been communicated to third parties, notification to the latter of the rectification, erasure or blocking;

8 to have a judicial remedy if the rights guaranteed in this article are infringed.

Article 15—Exceptions to the Data Subject's Right of Access to Public-sector Files

1 The member states may limit by statute the rights provided for in points 3 and 4 of Article 14 for reasons relating to:

(a) national security; or

(b) defense; or

(c) criminal proceedings; or

(d) public safety; or

(e) a duly established paramount eco-

nomical and financial interest of a member state or of the European Communities; or

(f) the need for the public authorities to perform monitoring or inspection functions; or

(g) an equivalent right of another individual and the rights and freedoms of others.

2 In the circumstances referred to in paragraph 1 the supervisory authority shall be empowered to carry out, at the request of the data subject, the necessary checks on the file.

3 The member states may place limits on the data subject's right of access to data compiled temporarily for the purpose of extracting statistical information therefrom.

Chapter V—Data Quality

Article 16—Principles

1 The member states shall provide that personal data shall be:

(a) collected and processed fairly and lawfully;

(b) stored for specified, explicit and lawful purposes and used in a way compatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

(d) accurate and, if necessary, kept up to date; inaccurate or incomplete data shall be erased or rectified;

(e) kept in a form which permits identification of the data subjects for no longer than is necessary for the purpose for which the data are stored.

2 It shall be for the controller of the file to ensure that paragraph 1 is complied with.

Article 17—Special Categories of Data

1 The member states shall prohibit the automatic processing of data revealing

ethnic or racial origin, political opinions, religious or philosophical beliefs or trade-union membership, and of data concerning health or sexual life, without the express and written consent, freely given, of the data subject.

2 The member states may, on important public-interest grounds, grant derogations from paragraph 1 on the basis of a law specifying the types of data which may be stored and the persons who may have access to the file and providing suitable safeguards against abuse and unauthorized access.

3 Data concerning criminal convictions shall be held only in public-sector files.

Article 18—Data Security

1 The member states shall provide in their law that the controller of a file shall take appropriate technical and organizational measures to protect personal data stored in the file against accidental or unauthorized destruction or accidental loss and against unauthorized access, modification or other processing.

Such measures shall ensure in respect of automated files an appropriate level of security having regard to the state of the art in this field, the cost of taking the measures, the nature of the data to be protected and the assessment of the potential risks. To that end, the controller of the file shall take into consideration any recommendations on data security and network interoperability formulated by the commission in accordance with the procedure provided for in Article 29.

2 Methods guaranteeing adequate security shall be chosen for the transmission of personal data in a network.

3 In the event of online consultation the hardware and software shall be designed in such a way that the consultation takes place within the limits of the authorization granted by the

controller of the file.

4 The obligations referred to in paragraphs 1, 2 and 3 shall also be incumbent on persons who, either *de facto* or by contract, control the operations relating to a file.

5 Any person who in the course of his work has access to information contained in files shall not communicate it to third parties without the agreement of the controller of the file.

Chapter VI—Provisions Specifically Relating to Certain Sectors

Article 19

The member states may grant in respect of the press and the audiovisual media derogations from the provisions of this directive insofar as they are necessary to reconcile the right to privacy with the rules governing freedom of information and of the press.

Article 20

The member states shall encourage the business circles concerned to participate in drawing up European codes of conduct or professional ethics in respect of certain sectors on the basis of the principles set forth in this directive.

Chapter VII—Liability and Sanctions

Article 21—Liability

1 The member states shall provide in their law that any individual whose personal data have been stored in a file and who suffers damage as a result of processing or of any act incompatible with this directive shall be entitled to compensation from the controller of the file.

2 The member states may provide that the controller of the file shall not be

liable for any damage resulting from the loss or destruction of data or from unauthorized access if he proves that he has taken appropriate measures to fulfill the requirements of Articles 18 and 22.

Article 22—Processing on Behalf of the Controller of the File

1 The member states shall provide in their law that the controller of the file must, where processing is carried out on his behalf, ensure that the necessary security and organizational measures are taken and choose a person or enterprise who provides sufficient guarantees in that respect.

2 Any person who collects or processes personal data on behalf of the controller of the file shall fulfill the obligations provided for in Articles 16 and 18 of this directive.

3 The contract shall be in writing and shall stipulate, in particular, that the personal data may be divulged by the person providing the service or his employees only with the agreement of the controller of the file.

Article 23—Sanctions

Each member state shall make provision in its law for the application of dissuasive sanctions in order to ensure compliance with the measures taken pursuant to this directive.

Chapter VIII—Transfer of Personal Data to Third Countries

Article 24—Principles

1 The member states shall provide in their law that the transfer to a third country, whether temporary or permanent, of personal data which are undergoing processing or which have been gathered with a view to processing may

take place only if that country ensures an adequate level of protection.

2 The member states shall inform the commission of cases in which an importing third country does not ensure an adequate level of protection.

3 Where the commission finds, either on the basis of information supplied by member states or on the basis of other information, that a third country does not have an adequate level of protection and that the resulting situation is likely to harm the interests of the Community or of a member state, it may enter into negotiations with a view to remedying the situation.

4 The commission may decide, in accordance with the procedure laid down in Article 30(2) of this directive, that a third country ensures an adequate level of protection by reason of the international commitments it has entered into or of its domestic law.

5 Measures taken pursuant to this article shall be in keeping with the obligations incumbent on the Community by virtue of international agreements, both bilateral and multilateral, governing the protection of individuals in relation to the automatic processing of personal data.

Article 25—Derogation

1 A member state may derogate from Article 24(1) in respect of a given export on submission by the controller of the file of sufficient proof that an adequate level of protection will be provided. The member state may grant a derogation only after it has informed the commission and the member states thereof and in the absence of notice of opposition given by a member state or the commission within a period of ten days.

2 Where notice of opposition is given the commission shall adopt appropriate measures in accordance with the procedure laid down in Article 30(2).

Chapter IX—Supervisory Authorities and Working Party on the Protection of Personal Data

Article 26—Supervisory Authority

1 The member states shall ensure that an independent competent authority supervises the protection of personal data. The authority shall monitor the application of the national measures taken pursuant to this directive and perform all the functions that are entrusted to it by this directive.

2 The authority shall have investigative powers and effective powers of intervention against the creation and exploitation of files which do not conform with this directive. To that end it shall have, *inter alia*, the right of access to files covered by this directive and shall be given the power to gather all the information necessary for the performance of its supervisory duties.

3 Complaints in connection with the protection of individuals in relation to personal data may be lodged with the authority by any individual.

Article 27—Working Party on the Protection of Personal Data

1 A Working Party on the Protection of Personal Data is hereby set up. The working party, which shall have advisory status and shall act independently, shall be composed of representatives of the supervisory authorities, provided for in Article 26, of all the member states and shall be chaired by a representative of the commission.

2 The secretariat of the Working Party on the Protection of Personal Data shall be provided by the commission's departments.

3 The Working Party on the Protection of Personal Data shall adopt its own rules of procedure.

4 The Working Party on the Protection of Personal Data shall examine

questions placed on the agenda by its chairman, either on his own initiative or at the reasoned request of a representative of the supervisory authorities, concerning the application of the provisions of Community law on the protection of personal data.

Article 28—Tasks of the Working Party on the Protection of Personal Data

1 The Working Party on the Protection of Personal Data shall:

(a) contribute to the uniform application of the national rules adopted pursuant to this directive;

(b) give an opinion on the level of protection in the Community and in third countries;

(c) advise the commission on any draft additional or specific measures to be taken to safeguard the protection of privacy.

2 If the Working Party on the Protection of Personal Data finds that significant divergences are arising between the laws or practices of the member states in relation to the protection of personal data which might affect the equivalence of protection in the Community, it shall inform the commission accordingly.

3 The Working Party on the Protection of Personal Data may formulate recommendations on any questions concerning the protection of individuals in relation to personal data in the Community. The recommendations shall be recorded in the minutes and may be transmitted to the Advisory Committee referred to in Article 30. The commission shall inform the Working Party on the Protection of Personal Data of the action it has taken in response to the recommendations.

4 The Working Party on the Protection of Personal Data shall draw up an annual report on the situation regarding the protection of individuals in relation to the processing of personal data in the Community and in third countries,

which it shall transmit to the commission.

Chapter X—Rule-making Powers of the Commission

Article 29—Exercise of Rule-making Powers

The commission shall, in accordance with the procedure laid down in Article 30(2), adopt such technical measures as are necessary to apply this directive to the specific characteristics of certain sectors having regard to the state of the art in this field and to the codes of conduct.

Article 30—Advisory Committee

1 The commission shall be assisted by a Committee of an advisory nature composed of the representatives of the member states and chaired by a repre-

sentative of the commission.

2 The representative of the commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter, if necessary by taking a vote. The opinion shall be recorded in the minutes. In addition, each member state shall have the right to ask to have its position recorded in the minutes. The commission shall take the utmost account of the opinion delivered by the committee. It shall inform the committee of the manner in which its opinion has been taken into account.

Final Provisions

Article 31

1 The member states shall bring into force the laws, regulations and adminis-

trative provisions necessary for them to comply with this directive by January 1, 1993.

The provisions adopted pursuant to the first subparagraph shall make express reference to this directive.

2 The member states shall communicate to the commission the texts of the provisions of national law which they adopt in the field covered by this directive.

Article 32

The commission shall report to the council and the European Parliament at regular intervals on the implementation of this directive, attaching to its report, if necessary, suitable proposals for amendments.

Article 33

This directive is addressed to the member states.

Privacy Committee's Recommended Data Protection Principles

Note: These principles are based on the Commonwealth Information Privacy Principles contained in the Privacy Act 1988. Text which appears in italics is not in the Commonwealth Act. The changes have been made to take into account recent international developments in data protection, in particular the European Commissions draft directive (Appendix 3).

Principle 1

Manner and purpose of collection of personal information

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:
 - (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
 - (b) the collection of the information is necessary for or directly related to that purpose.
2. Personal information shall not be collected by a collector by unlawful or unfair means.

Principle 2

Solicitation of personal information from individual concerned

1. *Personal information shall be solicited directly from the individual concerned except where the individual authorises otherwise, or where personal information may be disclosed to the collector in accordance with these Principles or a Code of Practice under this Act.*
2. Where:
 - (a) a collector collects personal information for inclusion in a record or in a generally available publication; and
 - (b) the information is solicited by the collector from the individual concerned;

the collector 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 *informed* of:

- (c) the purpose for which the information is being collected;
- (d) if the collection of the information is authorised or required by or under law - the fact that the collection of the information is so authorised or required;
- (e) *the mandatory or voluntary nature of the information collection and the effects on the individual concerned, if any, of not providing all or any part of the requested information;*
- (f) *the existence of the right of access to and rectification of the data relating to the individual;*
- (g) *the name and address of the recordkeeper;*
- (h) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first mentioned person, body or agency to pass on that information.

Principle 3

Solicitation of personal information generally

Where:

- (a) a collector collects personal information for inclusion in a record or in a generally available publication; and
- (b) the information is solicited by the collector;

the collector shall take 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, *not excessive*, and is *accurate*, 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 4

Storage and security of personal information

A recordkeeper who has possession or control of a record that contains personal information shall ensure *that the personal information is:*

- (a) *stored for specified, explicit and lawful purposes and used in a way consistent with those purposes;*
- (b) *adequate, relevant, and not excessive in relation to the purposes for which it is stored;*
- (c) *processed fairly and lawfully;*
- (d) *kept for no longer than is necessary for the purposes for which the information is stored;*
- (e) personal information is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and
- (f) if it is necessary for the *personal information* to be given to a person in connection with the provision of a service to the recordkeeper, everything reasonably within the power of the recordkeeper is done to prevent unauthorised use or disclosure of *the information*.

Principle 5

Information relating to records kept by recordkeeper

1. A recordkeeper who has possession or control of records that contain personal information shall, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:
 - (a) whether the recordkeeper has possession or control of any records that contain personal information; and
 - (b) *whether the recordkeeper has possession or control of such a record relating to that person; and*
 - (c) if the recordkeeper has possession or control of a record that contains such information:
 - i) the nature of that information;
 - ii) the main purposes for which the information is used; and
 - iii) the steps that the person should take if the person wishes to obtain access to the record.
2. A recordkeeper is not required under clause 1 of the Principle to give a person information if the recordkeeper is required or authorised to refuse to give that information to the person under the applicable provisions of any law of *New South Wales* that provides for access by persons to documents.

3. A recordkeeper shall maintain a record setting out:
 - (a) the nature of the records of personal information kept by or on behalf of the recordkeeper;
 - (b) *the sources of personal information contained in those records;*
 - (c) *the purpose for which the information was collected and the authority for that collection;*
 - (d) the purpose for which each type of record is kept;
 - (e) the classes of individuals about whom records are kept;
 - (f) the period for which each type of record is kept;
 - (g) the persons who are entitled to have access to personal information contained in the records and the conditions under which they are entitled to have that access; and
 - (h) the steps that should be taken by persons wishing to obtain access to that information.
4. A recordkeeper shall:
 - (a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and
 - (b) give the Commissioner, in the month of June in each year, a copy of the record so maintained.

Principle 6

Access to records containing personal information

1. Where a recordkeeper has possession or control of a record that contains personal information, the individual concerned shall, *without excessive delay or expense*, be entitled to have access to that record, except to the extent that the recordkeeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of *New South Wales* that provides for access by persons to documents.

Principle 7

Alteration of records containing personal information

1. A recordkeeper who has possession or control of a record that contains personal information shall take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

- (a) is accurate; and
 - (b) is, 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, relevant, up-to-date, complete and not misleading.
2. *Where personal information has been corrected, deleted or added to in accordance with clause 1, the individual concerned shall be entitled to have recipients of that information notified of the alterations by the recordkeeper.*
 3. The obligation imposed on a recordkeeper by clause 1 is subject to any applicable limitation in a law of *New South Wales* that provides a right to require the correction or amendment of documents.
 4. Where:
 - (a) the recordkeeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and
 - (b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of *New South Wales*;

the recordkeeper shall, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Principle 8

Recordkeeper to check accuracy etc. of personal information before use

A recordkeeper who has possession or control of a record that contains 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 *relevant* accurate, up to date and complete.

(Commonwealth Principle 9 has been deleted as it is effectively incorporated into Principle 8 by addition of the word "relevant". Commonwealth Principle 9 states:

A recordkeeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant).

Principle 9

Limits on use of personal information

1. A recordkeeper who has possession or control of a record that contains personal information shall not use the information for a *purpose other than that for which it was collected and which was specified in accordance with Principle 5* unless:

- (a) the individual concerned has consented to use of the information for that other purpose;
- (b) the recordkeeper 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 person; or
- (c) use of the information for that other purpose is required or authorised by or under law.

(Parts (d) and (e) of the Commonwealth's IPP 10 have been deleted. Derogations from the statements of principle should be dealt with in either the Codes of Conduct or specific legislative provisions relating to the recordkeeper).

Principle 10

Limits on disclosure of personal information

1. A recordkeeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:
 - (a) the individual concerned *has been informed* under Principle 2, that information of that kind is usually passed to that person, body or agency;
 - (b) the individual concerned has consented to the disclosure;
 - (c) the recordkeeper 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 of another person;
 - (d) the disclosure is required or authorised by or under law.
2. A person, body or agency to whom personal information is disclosed under clause 1 of this Principle shall not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

Parts 1(d) and (e) and 2 of the Commonwealth's IPP 11 have been deleted for the same reason as deletions were made to the previous principle.

New Principle 11

1. *Notwithstanding Principles 9 and 10 information relating to ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life shall not be used or disclosed by a recordkeeper without the express written consent, freely given, of the individual concerned.*
2. *Information relating to an individual's criminal history may only be processed as required or authorised by law or a Code of Practice under this Act.*