

https://dspace.org/

Policy for managing access to intelligence information in post-apartheid South Africa

Africa, Sandra Elizabeth

2008-03-10T12:27:41Z
http://hdl.handle.net/10539/4617

Downloaded from a DSpace repository. https://dspace.org/

POLICY FOR MANAGING ACCESS TO INTELLIGENCE INFORMATION IN POST-APARTHEID SOUTH AFRICA

Submitted by Sandra Elizabeth Africa

In fulfilment of the requirements for the degree

PhD in Management

University of the Witwatersrand

Supervisor: Professor Gavin Cawthra

September 2006

TABLE OF CONTENTS

	Pages
DECLARATION.....	**v**
ABSTRACT……	**vi**
TABLE OF ACRONYMS…….	**vii**
CHAPTER 1: AIM OF THE STUDY ……..	**1**
Problem statement……	1
Background……...	1
Aim of the study…… .	3
The research questions……..	5
Significance of the study……..	7
Scope of the study……	9
Title of the dissertation……	12
Structure of the dissertation…….	13
CHAPTER 2: METHODOLOGY……	**15**
Introduction…….	15
Main methodological features of the study…….	16
Underlying assumptions of the study……..	20
The research process……	22
The research tools……	24
Interpretation of the research results……	28
Concluding remarks…….	30
CHAPTER 3: LITERATURE REVIEW ……..	**31**
Introduction…….	31
Conceptual approaches to secrecy……..	31
Balancing secrecy and access to information in international relations…….	35
Secrecy and transparency in liberal democracies……...	39

Secrecy and transparency in societies in transition…… 42
Secrecy and transparency in South Africa……. 49
The national security debate and its implications for security sector governance……. 52
National security in Africa and the Third World……. 56
National security, security sector reform and access to information in South Africa…….. 60
Concluding remarks…….. 63

CHAPTER 4: OFFICIAL SECRECY AND STATE SECURITY UNDER MINORITY RULE IN SOUTH AFRICA ……. 66
Introduction…….. 66
The period prior to 1910…….. 67
1910 – 1948……. 70
1945 – 1960……. 74
1960 – 1976……. 77
1976 – 1990…….. 82
Concluding remarks…… 87

CHAPTER 5: THE TRANSITION TO DEMOCRACY, AND ITS IMPLICATIONS FOR INTELLIGENCE ACCOUNTABILITY AND TRANSPARENCY…….. 90
Introduction…….. 90
The context of negotiations for changes in the intelligence services…… 90
The management of intelligence information during the negotiations phase (1990-1993)…… 93
The management of intelligence information under the Transitional Executive Council (June 1993- April 1994)…… 97
The management of intelligence information under the RSA Constitution of 1993 (the "Interim Constitution") from May 1994 - December 1994……. 100
Impact of the Constitution of the Republic of South Africa, 1996 on the intelligence services……. 107
Parliamentary oversight and access to information……. 109

The role of the Inspector-General of Intelligence…….. 111
The role of the Auditor-General…… 112
Concluding remarks…… 116

CHAPTER 6: IMPLICATIONS OF THE PROMOTION OF ACCESS TO INFORMATION ACT, 2000 FOR THE SOUTH AFRICAN INTELLIGENCE SERVICES …….. 118
Introduction…… 118
The policy and legislative context of the PAIA……. 118
Assessment of the post-apartheid legislative context for secrecy…….. 122
Origins for the Promotion of Access to Information Act, 2000…… 124
Outline of the Act…….. 127
Scope of application of the Act……. 127
Routine disclosures required to be contained in the PAIA manuals…… 129
Requests for access to information……. 130
Grounds for refusal of access to records……. 130
Implications of the grounds for refusal for the intelligence services…….. 131
Appeals…….. 139
Functions of the Human Rights Commission…… 139
Other aspects covered in the Act…… 139
Implications of the overall legal framework for secrecy and transparency…… 140
Comparative international experience…… 140
United States of America (USA)…… 142
Canada…… 146
India……. 149
Lessons for South Africa from the international examples…….. 152
Concluding remarks…….. 154

CHAPTER 7: APPLICATION OF THE PROMOTION OF ACCESS TO INFORMATION ACT, 2000, IN THE INTELLIGENCE SERVICES UP UNTIL AUGUST 2005…… 156
Overview of implementation of the Act…….. 156
Capacity of the intelligence services for implementation of the PAIA…….. 158

Compliance by the intelligence services with the provisions of the PAIA…… 160
Case Studies…… 166
South African History Archives Trust (SAHA) applications to the NIA
and the Department of Justice and Constitutional Development (DOJ)
for access to TRC records…… 166
CCII Systems (Pty) Ltd vs the Minister of Defence on the release of
records relating to the government's Strategic Arms Procurement Package…. 178
Concluding remarks……. 185

CHAPTER 8: ANALYSIS OF THE RESEARCH RESULTS……. 188
Introduction ……. 188
Managing intelligence information in the transition…… 189
Implications of the key issues in the literature……. 190
Interpreting the interview results…….. 193
Other countries' experiences…… 196
Policy recommendations…….. 197
Principles for the classification and declassification of information…… 201
Various scenarios requiring policy on classification and declassification …….. 203
Concluding remarks…… . 209

INTERVIEWS ……. .. 214

TABLES:
Table 1. Summary of classification of TRC records, in Affidavit filed by
D. Porogo in High Court (TPD) on 22 December 2003……. 172

REFERENCES…….. 216

DECLARATION

I declare that this report is my own, unaided work. It is submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy, at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in any other University.

_____

Sandra Elizabeth Africa

ABSTRACT

Under apartheid, the South African intelligence services operated in secrecy and without the framework of a Constitution upholding basic human rights. The situation changed drastically with the introduction of a democratic political dispensation in 1994, and with the adoption of the Republic of South Africa Constitution Act, 1996. One of the fundamental rights contained in the Bill of Rights (Chapter 2 of the Constitution) was the right of access to information. The subsequent passage of legislation to give effect to this right, required all state structures - including the civilian intelligence services, the National Intelligence Agency and the South African Secret Service - to actively disclose information about themselves, and to receive and respond to requests for access to records that were made in terms of the enabling legislation.

The main issue with which the study is concerned - the balance between secrecy and transparency in a democracy - is one of a wider set of concerns related to democratic control and accountability of the intelligence and security services. The study explores policy options for reconciling the public's right to information with the intelligence services' need for a degree of secrecy with which to conduct their work. Inter alia, it compares the policy choices of three countries about how their intelligence services should function in relation to access to information legislation.

The research reveals that there was uneven and erratic compliance by the intelligence services with key provisions of the Promotion of Access to Information Act, 2000, up to and including August 2005. The weaknesses arose because of the absence of clear policy on how to implement the Act in relation to the intelligence services, and in relation to information held by the intelligence and security services.

The study therefore argues the need for a comprehensive policy package, which sets criteria for the conditions under which information should be protected from disclosure, and the criteria for determining when information no longer requires such protection. Finally, it argues for strict oversight of the intelligence services' choices around secrecy and transparency.

TABLE OF ACRONYMS

AC	Amalgamation Committee
ADS	African Defence Systems (Pty) Ltd
ANC	African National Congress
AU	African Union
BOSS	Bureau for State Security
CCII	CCII Systems (Pty) Ltd
CDAF	Geneva Centre for the Democratic Control of Armed Forces
CDRC	Classification/Declassification Review Committee
CIA	Central Intelligence Agency
CODESA	Convention for a Democratic South Africa
COMSEC	Electronic Security Communications (Pty) Ltd, 2002
CSIS	Canadian Security Intelligence Service
DOD	Department of Defence
DOJ	Department of Justice and Constitutional Development
DIO	Deputy Information Officer

DIS	Department of Intelligence and Security
DMI	Directorate of Military Intelligence
DMI	Division of Military Intelligence
ECOWAS	Economic Community of West African States
EU	European Union
FOIA	Freedom of Information Act
GCHQ	Government Communications Headquarters
GFC	German Frigate Consortium
HOCS	Heads of Civilian Services
HRC	Human Rights Commission
IAAC	Information Act Advisory Committee
ICCPR	International Covenant on Civil and Political Rights
ICD	Intelligence Coordination Division
IO	Information Officer
IPU	Inter-Parliamentary Union
ISDSC	Inter-state Defence and Security Committee
ISSUP	Institute for Strategic Studies, University of Pretoria

IRC	Interdepartmental Review Committee
JCIC	Joint Coordinating Intelligence Committee
JSCI	Joint Standing Committee on Intelligence
MISS	Minimum Information Security Standards
NEPAD	New Partnership for Africa's Development
NIA	National Intelligence Agency
NCC	National Communications Centre
NICOC	National Intelligence Coordinating Committee
NIS	National Intelligence Service
NSA	National Security Agency
NSMS	National Security Management System
OAU	Organisation of African Unity
OB	Ossewa Brandwag
PAB	Placement Advisory Board
PAC	Pan Africanist Congress
PAIA	Promotion of Access to Information Act, 2000

PFMA	Public Finance Management Act, 1999
PKO	Peacekeeping Operation
PMC	Political and Military Council
RCMP	Royal Canadian Mounted Police
RIS	Republican Intelligence Service
RSA	Republic of South Africa
SACP	South African Communist Party
SADC	Southern African Development Community
SADF	South African Defence Force
SAHA	South African History Archive
SANAI	South African National Academy of Intelligence
SANDF	South African National Defence Force
SAP	South African Police
SAPS	South African Police Service
SASS	South African Secret Service
SIRC	Security Intelligence Review Committee
SSAC	State Security Advisory Council

SSC	State Security Council
TBVC	Transkei, Bophutatswana, Venda, Ciskei
TEC	Transitional Executive Council
TRC	Truth and Reconciliation Commission
UDF	Union Defence Force
UK	United Kingdom
UN	United Nations
UNDP	United Nations Development Programme
UNITA	National Union for the Total Independence of Angola
US	United States
USA	United States of America
USSR	Union of Soviet Socialist Republics
WHAM	Winning Hearts and Minds

CHAPTER ONE

AIM OF THE STUDY

Problem statement

In 1994, South Africa emerged from a period of minority rule that had been characterised by excessive government secrecy and the denial of basic human rights. One such right was the right of access to information held and generated by the state. Whilst there has been a dramatic increase in governmental transparency since 1994, policy makers of the new political order have not reflected adequately on the implications of transparency for the intelligence services.

As a result of this policy vacuum, the post-apartheid intelligence services have been ambivalent and inconsistent in applying the constitutional principle and legislation giving effect to the right of access to information. Members of the public therefore, do not enjoy the full benefits of this right, and from time to time find themselves at odds with the state. This state of tension is likely to persist until clear policy guidelines for the management of different categories of records held by the intelligence services are formulated and made known. Given the secrecy surrounding the intelligence services, and the potential for abuse that such secrecy carries, it is imperative that citizens be assured that there are clear parameters and policy guidelines for the exercise of secrecy and transparency.

Background

Prior to 1994, the legislative environment provided the conditions for the South African security services to conduct their affairs with virtually no public scrutiny. The Official Secrets Acts of 1912 and later 1956, the Security Intelligence and State Security Council Act (Act 64 of 1972), the Bureau for State Security Act, 1978 (Act 104 of 1978), the Protection of Information Act, 1982 (Act 84 of 1982), and various laws relating to the financing of the security services, all served to establish a veil of secrecy around the security services (Mathews, 1978; Africa, 1992).

The Constitution of the Republic of South Africa, 1996 (Act 108 of 1996) introduced a Bill of Rights and established a number of institutions to support the constitutional democracy. These included a Public Protector, the Human Rights Commission, the Commission for Gender Equality, the Commission for the Promotion and Protection of the Rights of Cultural, Religious and Linguistic Communities, the Auditor-General and the Independent Electoral Commission (RSA Constitution, 1996, Chapter 9).

Since the enactment of the Constitution, there have been extensive legislative changes aimed at achieving alignment with the Constitution. Hundreds of apartheid era laws have been repealed, and new legislation has come into effect. In some laws, provision has been made for institutions that will promote and uphold the rights contained in the Bill of Rights. For example, arising out of a constitutional provision, the Intelligence Services Control Act, 1994 (Act 40 of 1994) provides for the establishment of a multi-party parliamentary oversight committee, and for the appointment of Inspectors-General for the intelligence services to investigate complaints from members of the public.

South Africa's open democracy confronted government with several challenges, including that of adequate balancing the requirements of an open democracy, with the revised functions of the security services. Strong political leadership and vigorous oversight would be required to ensure that the fledgling intelligence services, themselves the product of a sensitive transition, interpreted their legislative mandates correctly, and acted in accordance with the spirit of the Constitution.

The Constitution stipulated that national legislation be instituted to give effect to the right of access to information. In line with this requirement, the Promotion of Access to Information Act, 2000 (Act 2 of 2000) was passed. These statutes have challenged state security organs to actively disclose information about themselves, and to receive and respond to requests for access to records. Notwithstanding a broadened and people-centred concept of security having been written into the new constitutional dispensation, some observers argue that the security services continue to resist disclosure of information, in this way undermining the constitutional principle of access to information (Harris, 2002; Currie & Klaaren, 2002).

There are considerable capacity challenges in gearing the post-apartheid intelligence services towards dispensing their constitutional obligations for implementing the Promotion of Access to Information Act, 2000. The Act is a relatively complex piece of legislation, the implementation of which requires the production of manuals, a capacity on the part of public and private bodies to respond in a timely fashion to requests for access to records, their ability to process appeals, alongside the role of the courts which must become involved when requesters wish to seek recourse to justice, and compliance with a system of annual reporting (McKinley, 2004). These requirements will be explained in more detail later in the study. What will also be addressed, at that point, is the capacity displayed by the intelligence services to respond to comply with the Act, up till August 2005, and whether there was adequate policy to guide the services in fulfilling their duty of compliance.

Aim of the study

The aim of this study is to explore appropriate policy guidelines for managing public access to intelligence information in post-apartheid South Africa, and by implication, policy guidelines for regulating state secrecy, particularly secrecy that is invoked in the name of national security. In so doing, the study questions whether the post- apartheid intelligence services are in practice, significantly more transparent and publicly accountable than their apartheid-era predecessors. My observation is that there has been at best, considerable ambiguity on the part of the intelligence services and other policy actors, about how to pursue appropriate and meaningful levels of transparency in the intelligence environment, and under what conditions the resort to secrecy can be constitutionally invoked. A more pessimistic analysis would suggest that there appears to have been significant continuity with the apartheid past in the manner in which the intelligence services and policy makers have retreated into justifications of their secrecy, even where no real threat to national security would have been posed by their opting for greater openness and public disclosure. I attempt to describe, understand and explain this ambivalence, and to present policy alternatives that will compromise neither the intelligence services' execution of their mandate, nor the right of access of members of the public to information held by the state. For government, developing such policy requires the careful management of the tensions inherent in the relationship between democracy and secrecy (Mathews, 1978; Lustgarten & Leigh, 1994; Levy, 2004)

My departure point in evaluating the merits of secrecy and transparency in the management of intelligence information is that neither secrecy nor transparency is inherently good nor bad for governance of entities such as the intelligence services, but should be assessed in the context of how they are exercised or managed. It is assumed that the intelligence services of post-apartheid South Africa were established with the noble intention of upholding the Constitution.

Levy (2004:144) points to the White Paper on Intelligence passed by South Africa's first democratic parliament to illustrate this:

> The White Paper (introduced in 1995) referred to the role of the intelligence community in protecting the Reconstruction and Development Programme (RDP), the macro-economic policy adopted to kick-start the transformation to democracy. Although stability could be achieved within a totalitarian state, the political culture elaborated in the White Paper clearly indicates that the aim is stability within the framework of a constitutional democracy. In that light, the role of the intelligence services as instruments of democracy can, in the broadest sense, be explained by the responsibility these structures have towards the protection of democratic principles, such as the right to the means of life, human rights, freedom and the rule of law.

This study accepts as a departure point that the post-apartheid South African intelligence services are guided in their conduct by, inter alia, the constitutional provision of access to information, and the passing of legislation to give effect to the right of access to information stipulated in the country's Constitution. Any inconsistencies in their conduct are flaws seeking to be aligned with this greater objective.

The research questions

Early on, the study explores the roots of official secrecy in South Africa, as a basis for understanding whether these have influenced the institutional framework of secrecy in post-apartheid South Africa. It traces the political imperatives that caused successive South African governments, in the course of the twentieth century, to introduce legislation that ensured their continued dominance over the country's black majority (Mathews, 1971, 1978; Geldenhuys, 1984; Seegers, 1996). The study also reviews the management of intelligence information in the period during which the country's negotiated settlement gave rise to a new intelligence dispensation. What is at issue is whether the post-apartheid intelligence services, which operate under a democratic Constitution, are adversely affected by aspects of the legislative and regulatory regime under which they function. Some writers have argued that the fact that some aspects of this regime date back to the apartheid era, have created the conditions for the intelligence services to overlook or fall short of their constitutional obligations (Currie & Klaaren, 2002; McKinley, 2004). The study therefore attempts to assess these claims.

A second question concerns the impact of the seemingly contradictory policy, legislative and regulatory arrangements under which the intelligence services function, on the public's access to information. The main contradiction is that within post-apartheid South Africa, there is both a constitutionally defined right of public access to information and provision for some organs of the state (notably the intelligence services) to conduct their affairs in relative secrecy (Currie & Klaaren, 2002). For example, the Intelligence Services Act, 2002 requires the heads of the intelligence services to protect the identities of members, sources and methods of collection (Qunta, 2004). Another example is that the Protection of Information Act, 1982 which has coexisted since the year 2000 with the Promotion of Access to Information Act, 2000, provides penalties for disclosure of, or unauthorised access to a much wider spectrum of information and records than contemplated in the latter Act (Currie & Klaaren, 2002). A third example is that the National Archives Act, 1996, whilst providing for declassification of records after the lapse of a twenty year period, is silent on how records whose contents may originally have been classified secret, on grounds of national security, are to be handled after the twenty year period (McKinley, 2004).

In addition there is a Cabinet guideline, the Minimum Information Security Standards (MISS), which guides officials in the day-to-day security classification of information. What is cause for concern is that the MISS requires state officials across government departments, without regard for their levels of authority or responsibility in the bureaucracy, to implement and adhere to prescribed secrecy measures, without any oversight mechanisms regulating their actions. Officials are required and permitted in terms of the MISS, to routinely classify "sensitive" information as "Top Secret", "Secret", "Confidential" or "Restricted" depending on the perceived degree of harm to national security that disclosure of information thus classified would result in (Currie & Klaaren, 2002). The criteria for classification of records, and therefore for withholding information from the public, are not contained in legislation, creating concern that the MISS is in fact in contradiction to the Promotion of Access to Information Act, 2000. The study explores the implications of these gaps in the legislative and policy framework, and recommends options for addressing the inconsistencies in order to provide for a more consistent policy environment.

A third question raised is whether custodianship of intelligence records under the post-apartheid dispensation is regulated in a manner that is sufficient to guarantee their integrity and ensure that the records will exist in future, as an adequate reflection of the truth. This concern is particularly germane to information – and records – about the intelligence services, because they are generally closed to public scrutiny (Posel & Simpson, 2002). Those who are recruited into the intelligence services are sworn to secrecy and may not disclose their activities; only a limited amount of information about the day-to-day priorities and activities of these structures is released to the public, and even oversight bodies entrusted with ensuring that the intelligence services act within legitimate norms are often not at liberty to publicise all aspects of their interactions with these structures. The final report of the Truth and Reconciliation Commission (TRC) emphasised the need for the preservation of official records in post-apartheid South Africa, and exposed the reality that much of South Africa's officially recorded history had been destroyed in the final months of the apartheid government, as it sought to sanitise the record of its rule before a newly elected democratic government took power (Truth and Reconciliation Commission, 1998).

Finally, the study raises challenging policy questions generated by the access to information provisions of the Constitution and the legislation. These concern the nature of security threats

faced by South Africa, and the "classes" of intelligence information, that should, consequently, be subject to secrecy and protection. Another question concerns who should have the authority to classify information and in terms of what thresholds or standards. There is, more specifically, the challenge of finding a formula for how the records of the apartheid intelligence services should be preserved or handled, especially in the context of processes to encourage disclosure about human rights abuses committed by the apartheid security forces. This will probably be important for bringing closure to that period in the country's history. A final question concerns the duration of classification and the criteria for determining when a matter can be deemed to have lost its sensitivity and therefore its classified status. The public has concerns about the safeguards that exist to ensure that the declassification or classification of information is in the public interest.

Significance of the study

This study is relevant and timely for the following reasons:

First, South Africa is a relatively new democracy, and even though the intelligence services have been the subject of a fair amount of academic discussion and public debate, both in the period leading to the country's first democratic elections and afterwards (Southall, 1992; Breytenbach, 1992; Hough, 1992; Nhlanhla, 1992; Africa, 1992; Shaw, 1995; Henderson, 1998; Africa & Mlombile, 2001), it is in the detail that the debate needs to be elaborated. Much of the earlier writing reflected society's insistence on the need for vigilance against similar excesses to those experienced by the people at the hands of the security forces under white minority rule, under conditions of secrecy, and in the name of national security. There is a need to review the impact of policy and legislative directions of the new state, and to critique the performance of both state and non-state actors in realising the effectiveness of these. Where it is apparent that there are policy gaps, academic research can make an important contribution towards closing them.

Second, the study comes at a time when several democracies, facing grave threats in the form of terrorism, are contemplating restricting their citizens' civil liberties in the interests of national security (Todd & Bloch, 2003). For South African society, the debate is especially pertinent, given the reality that, having emerged from a past where human rights were

disregarded by the state, and successive white minority governments, any reversal or even qualification of the fundamental rights that are now provided for will be subject to the test of constitutionalism. The study recognises the human security underpinnings of the post-apartheid security dispensation, and attempts to find policy solutions within this paradigm.

A *third* reason that this study is significant is that the application of access to information takes place at a time when globalization, rapid technological development, and an information explosion expose just how vulnerable and penetrable the information systems of government really are. Communications technology has developed to such an extent – there is a multitude of satellite, digital and electronic possibilities - that most governments admit that they cannot guarantee that information they develop, store and communicate is not invulnerable to unauthorized access (Lipinski, 1999).

The failure to guarantee the integrity of their information systems affects the durability and effectiveness of secrecy regimens that governments might have in place, and calls into question the considerable funding that must go into physically securing information systems and personnel entrusted with information security. Another factor affecting the effectiveness of secrecy systems is globalization, and the growth of multinational governmental and private entities. This has given rise to a global scenario where identities are increasingly cast in transnational terms, where individual loyalty to a country might exist alongside or even be surpassed by identification with multinational corporate entities. The implications of this phenomenon - which is dramatically facilitated by the development of access to technology - is that people, while being defined as being of one or other territorial citizenship, are increasingly identifying with causes regardless of geographical boundaries that might separate them. In a technologically linked global environment, in a world where access to information is often the key to prosperity, and where territorial identities are being subsumed by other forms of identity, there are major challenges to be faced by policy makers who have to shape policy and develop appropriate policy for promoting and defending national security.

Last, the study is significant because it explores the interplay between a significant numbers of policy actors in giving effect to access to information policy. Apart from studying the available research material on the matter, the researcher conducted interviews with some of these actors, including officials in the intelligence services and other government

departments, technical drafters of the legislation promoting access to information, members of various oversight structures, academics, and representatives of non-governmental organisations. The data has helped to present the perspectives of various stakeholders. Understanding these perspectives is an important part of the policymaking process, which must seek to manage the tensions in the interests of the various stakeholders (Lee, 1991).

Scope of the study

The terminology and definitions used in this study, regarding South Africa's statutory security institutions, are derived from the Constitution of the Republic of South Africa (1996). Chapter 11 of the Constitution makes reference to "security services", consisting collectively of the national defence force, the police service, and the intelligence services. The actual shape, role and functions of the intelligence community were the product of much debate between the parties involved in negotiating South Africa's political future in the early 1990s (Africa, 1992; Nhlanhla, 1992; O'Brien, 1996).

One of the major departure points from the previous dispensation was to have two civilian intelligence services, one for domestic intelligence and another for foreign intelligence. As outlined in the White Paper on Intelligence adopted by the first democratic Parliament in 1994, and in the National Strategic Intelligence Act of 1994, the mission of the domestic intelligence service (the National Intelligence Agency, or NIA) was to conduct security intelligence within the borders of the Republic of South Africa in order to protect the Constitution. The overall aim was to ensure the security and stability of the state, and the safety and well being of its citizens.

In South African law, "domestic intelligence" means intelligence on any internal activity, factor or development that is detrimental to the national stability of the republic, or threats or potential threats to the constitutional order of the Republic and the safety and the well being of the people. The mission of the foreign intelligence service (the South African Secret Service, or SASS) was to conduct intelligence in relation to external threats, opportunities and other issues that might affect the Republic of South Africa, with the aim of promoting national security and the interests of the country and its people. The law defines "foreign

intelligence" as intelligence on any external threat or potential threat or potential threat to the national interests of the republic and its people, and intelligence regarding opportunities relevant to the protection and promotion of such national interests irrespective of whether or not it can be used in the formulation of the foreign policy of the Republic (RSA, National Strategic Intelligence Act, 1994).

This study does not address in detail the management of access to intelligence information held by the South African Police Service (SAPS), and the South African National Defence Force (SANDF), although the questions posed about civilian intelligence are equally relevant for these sectors of the security services, and although passing and illustrative references are made to this area. Indeed, there is room for broadening the analysis in this direction, not least because the intelligence community does straddle the defence and policing environments (Africa & Mlombile, 2001). This is made clear in the National Strategic Intelligence Act (Act 39 of 1994), which outlines the strategic intelligence-gathering mandates of the National Intelligence Agency, the South African Secret Service, Defence Intelligence in the South African National Defence Force, and Crime Intelligence within the South African Police Service.

My research focus is on policy alternatives for the management of *intelligence* information, defined for the purpose of the study, as records generated by the intelligence services in conducting their work. These records include the raw information documented and compiled from a number of "sources" e.g. informers, technical and signal collection points, written reports and analyses compiled by intelligence officers, and the assessments and reports generated out of such data, usually assessments of threats or perceived threats to national security that are typically presented to policy makers to inform decision-making (Richelson, 1989). They also include the dossiers or files on people and organisations that are the subject of intelligence gathering, and records relating to the methods used to gather the information.

My working definition of intelligence information also covers records relating to corporate governance of the intelligence services, including records about human resources management, and assets and financial management of the intelligence services. "Intelligence information" may or may not be highly sensitive (in other words, its public disclosure may or

may not have grave implications for national security), depending on the criteria and considerations that are brought to bear on its evaluation.

Whilst exploring policy alternatives for the management of intelligence information is the main focus of the study, I have attempted to locate it more broadly. Firstly, I have examined how state secrecy has evolved in twentieth century South Africa, especially under the apartheid rule of the National Party after 1948. The study provides an account of the legislative conditions that framed secrecy from one political era to the next, and the role played by the security and intelligence services under such conditions.

Another dimension of the study is to explore issues around the status, legitimacy and ownership of intelligence information in the country's movement from authoritarian to democratic rule. As a backdrop I have explained and provided an assessment of the political processes leading to the establishment of the new intelligence dispensation that saw the establishment of the NIA and the SASS. Both were to function under a changed set of political rules and my interest in this study is whether their founding and early development have seen their adaptation to these rules of accountability and regard for the Constitution and the law.

Finally, the research compares aspects of the experiences of countries that have attempted to grapple with the issues of maintaining a successful balance between transparency, secrecy and national security, in the management of their intelligence services. A notable feature, particularly in Western democracies, has been the existence of oversight mechanisms. These are an important part of a democracy's armoury against bureaucratic excess. Largely because of the accessibility of reading material on these jurisdictions, I have reviewed the United States of America (USA), Canada, and India as countries with oversight mechanisms as well as access to information legislative regimes. The management of information about repressive security forces that has filtered through various truth commissions may also be instructive (Hayner, 2001). While my choice of countries is neither exhaustive nor directly comparable to the South African experience, it does offer insights into how civil society and the security establishments in other countries have differed on the issues, and how the courts or policy makers have intervened to resolve the debates and demarcate the boundaries more clearly.

Title of the dissertation

The title of the dissertation is "Policy for managing access to intelligence information in post-apartheid South Africa". Managing policy, in this context, refers to the processes and choices made by decision makers and policy actors, around the provision of access to intelligence information. I attempt to analyse how, in post-apartheid South Africa all three tiers of government - the legislature, the Executive and the judiciary - as well as officials of the intelligence services, have defined their relationship to information generated by the intelligence services, by highlighting the choices they have made in relation to various challenges. The oversight structures created in terms of the Constitution and national legislation - the Auditor-General, the Joint Standing Committee on Intelligence (JSCI) and the Inspector-General for Intelligence - are three institutions that interact with the intelligence services based on their respective mandates. A brief overview of their record in accessing intelligence will be attempted. It is widely known, even accepted to an extent, that the intelligence services conduct much of their work in secret, giving rise to the central dilemma of this study: how credible policy can be set and implemented in a context where public scrutiny is limited (Lustgarten & Leigh, 1994). In the intelligence environment much information, even relatively innocuous information, finds itself beyond public scrutiny. The study attempts to address the implications of this condition, and to interrogate the imperatives which make it possible.

The discussion about "access to information" takes place in relation to the implementation of the constitutional principle guaranteeing the public right to information held by public and private bodies. As stated earlier, this constitutional principle, in the South African context, has been given legislative effect through the Promotion of Access to Information Act, 2000, which clearly spells out the conditions under which such access may be denied, a possibility provided for in the Constitution and the law. However, this Act co-exists with the Protection of Information Act, 1982, which was carried over from the apartheid period and, in the context of the Promotion of Truth and National Reconciliation Act, 1996, presents considerable challenges for the management of intelligence information in the transition to democracy.

Lastly, "post-apartheid South Africa" refers to South Africa after the first democratic elections in April 1994, a watershed in national politics. The elections ushered in a system of universal adult suffrage, multi-party political contestation, representative and accountable government, and independent institutions to safeguard the Constitution, which contained a Bill of Rights. This set of conditions did not materialise out of thin air, and for this reason, the study has examined the roots of secret service and the policy and legislative context in which it arises.

Structure of the dissertation

In Chapter One, I have set out the aims of the dissertation, outlining the research questions and providing the background that formed the basis for the study. These will be investigated in greater detail in the body of the dissertation.

The remainder of the dissertation covers the following areas:

- Chapter Two: in this chapter an outline of the methodology used in the study is provided;
- Chapter Three: this covers a review of the literature relevant to the study of public policy on secrecy and transparency in the governance of the intelligence services;
- Chapter Four: this chapter provides an overview of the history of official secrecy and the secret services in South Africa under minority rule till 1990;
- Chapter Five: this chapter reviews the management of access to intelligence information during the period of transition to a democratic political dispensation in South Africa;
- Chapter Six: this provides an analysis of the Promotion of Access to Information Act, 2000 and its implications for the South African intelligence services;
- Chapter Seven: this makes an assessment of the practical implementation of the Promotion of Access to Information Act, 2000 by the South African intelligence services, and
- Chapter Eight: this chapter provides an analysis of the research findings, and makes recommendations on policies to regulate the secrecy and transparency of the intelligence services in post-apartheid South Africa.

Implementing access to information legislation is a relatively new experience for South Africa, and it is particularly challenging in an area such as intelligence, which has traditionally been closed to public scrutiny. Balancing the role of the state in ensuring the

security and well-being of its citizens, and the constitutional right of access to information of the public is likely to involve difficult choices for the different policy actors in South African society. However, the country's history of unaccountable and secretive conduct on the part of the security services suggests there is no better alternative to striving to find the balance.

CHAPTER 2

METHODOLOGY

Introduction

In this chapter I explain the methodology used in the study. The previous chapter has explained the scope of the study. In summary, a broad historical account of secrecy under minority rule, especially under apartheid, lays the foundation for my analysis of the management of intelligence records during the transition, and in the post-apartheid era. This provides critical background information for my assessment of the capacity and willingness of the post-apartheid intelligence services to implement the constitutional and legislative requirement of access to information, and the role of various policy actors in shaping policy for the management of access to intelligence records. The study can be located within a broader policy concern, about the tension between secrecy and transparency in a democracy. After evaluating the concerns, actions or perspectives of various role-players about issues relating to access to information, the study puts forward policy alternatives for managing the tension between secrecy and transparency, in the case of the intelligence services, in a manner that is consistent with the Constitution, and the provisions of the Promotion of Access to Information Act, 2000.

A matter that must be confronted quite directly, is whether the Protection of Information Act, 1982 is unconstitutional, and whether the imperative for the state to protect categories of information, in the interests of national security, as currently provided for in law, can be reconciled with the provision of access to information, to the mutual satisfaction of a range of policy stakeholders. Exploring lessons from other democracies which have attempting to manage the tensions generated by secrecy – in particular the USA, Canada and India - I explore policy alternatives that can be considered in the South African context, around the

question of what information held by the state should be protected, at whose instance, and for how long.

I have already identified problem and research questions in Chapter One, and provided the background to the study. In this chapter, I briefly locate the study in the sphere of policy studies, and identify the assumptions from which I proceed. I outline the research process I followed, and the specific research tools I used to gather the data for the study. I describe how I synthesised and interpreted the data, striving to ensure that I did not become biased in the conclusions I reached. And finally, I applied the principles attendant to policy studies, by attempting to balance the interests of the various stakeholders in presenting what I considered to be viable policy alternatives.

Main methodological features of the study

The study essentially sets out to evaluate the success and depth of adherence to and implementation of the constitutional right of access to information, a right to which the public is generally entitled, even where the intelligence services of the country are concerned. My observation is that there are gaps in adherence to this requirement. Along with the Constitution, South Africa has an impressive array of legislation to underpin the new democratic order, but there are weaknesses in implementation in a range of key areas, where the interests of various stakeholders have to be managed. This is the challenge facing South Africa in the post-apartheid period, when a range of policy challenges face the government (De Coning, 2000).

Lee (1991) foresaw that the decade of the 1990s would be a period of major public policy change in South Africa, and that successful policy processes would have to be inclusive if they were to successfully assist the transition from authoritarian rule to democracy. He

pointed to a number of trends in the international development of policy studies which analysts could adopt in addressing policy issues. The first was that policy challenges were most successfully addressed if they were treated, not so much as problems requiring one-sided interventions by government, but as issues and trends which presented opportunities for civilian participation (Lee, 1991).

The second trend in policy studies that Lee (1991) pointed to is that policy studies were best undertaken for real clients, with real concerns in mind. Policy studies being pursued for their own sake were often hollow and of little use. A third trend was for the policy analyst to "create and explore all possible and some impossible options" (Lee, 1991:10). The reason for this was that policy making had to take into account a variety of interests, each propounding a view of the ideal policy outcome. The actual policy decision in all likelihood, would take into account the most valid concerns of the various stakeholders, making it advisable therefore, for the policy analyst to present a range of possibilities that appeal to all interested parties. Finally, Lee (1991) pointed out the trend that useful policy analysis was continually assessed for its impact and real-life consequences.

My research has been influenced by the approach outlined by Lee (1991). In the first place, the study of access to information and how the intelligence services should relate to this constitutional and legislative imperative, is a contemporary concern of the South Africa intelligence services, the government, political parties and non-governmental organisation, various oversight bodies and the South African public. My study has looked concretely at the available data on the implementation of the Act by the intelligence services, and the experience of various interest groups regarding this policy requirement. At issue in the study is a policy challenge – how much information to provide to the public, or how much information government is entitled to withhold from the public domain, depending on which way you look at it.

The study draws on a range of academic fields in attempting to achieve its goals. This is not unusual in the area of policy studies, and the fields of law, history, philosophy, politics and international relations have been drawn upon to explain and clarify different questions. Drawing on several disciplines is typical of the methodology of policy analysis which, according to Dunn (1994:2):

> draws from and integrates elements of multiple disciplines: political science, sociology, psychology, economics, and philosophy. Policy analysis is partly descriptive, drawing on traditional disciplines (for example, political science) that seek knowledge about causes and consequences of public policies. Yet policy analysis is also normative; an additional aim is the creation and critique of knowledge claims about the value of public policies for past, present and future generations.

Lee (1991:12) asserts further reasons for the eclectic nature of policy analysis:

> The first is the inability of any single model to 'explain' policy-making with its vast variety of conflicting actors and trends. …the second reason for an eclectic approach is inherent in the nature of public policy itself. It is the realisation that public policy-making is ultimately not a technical but a judgmental, value-making, value-asserting activity. The 'values' asserted by each policy maker will arise from a variety of sources: ideologies, political platforms, populist trends, even the personal convictions of policy analysts and advocates themselves.

Again, this view resonates with the study's approach. It was apparent that the concerns and value propositions of some of the actors I encountered were diametrically different. As an example, non-governmental organisations such as the South African History Archives (SAHA) were driven by a strong human rights ethic, whilst the heads of the intelligence

service were anxious to preserve their prerogative to conduct intelligence operations in secret, so as to deliver relevant and timely intelligence to the government. I set out to explore whether clear boundaries could be set to ensure that the intelligence services did not cross the line into the abyss of non-accountability. Yet there appeared to be an unspoken assumption that if left unchecked, the intelligence services would resort to unaccountable and possibly even unconstitutional behaviour reminiscent of the apartheid era (Harris, 2000; Currie & Klaaren, 2002).

This is a qualitative, rather than quantitative, study. It seeks to understand the tensions between two variables – secrecy and transparency – in the context of a constitutional democracy emerging from an authoritarian past, and still grappling with issues of a political transition. The data collection was therefore weighted heavily in favour of exploring the views, actions and responses of various policy actors. This is particularly so in the case of the case studies I have chosen, in order to demonstrate the contradictions and tensions displayed by various policy actors in their implementation of the requirements of the Promotion of Access to Information Act, 2000.

This attention to detailed description of the legislative regime under white minority rule is deliberate. It reflects my belief that without carefully clarifying the details, there can really be no informed analysis and interpretation of the success or otherwise with which any public policy is given effect to. I have, for example, traced the development of the system of governmental secrecy since before the time of Union, but more particularly since the advent of apartheid in 1948. A periodisation of the twentieth century has been useful in showing patterns and trends in secrecy. Because some elements of the secrecy framework have survived apartheid, I considered it necessary to understand their origins and to attempt to understand what power structures and relations they reinforce. I have also described in some detail, relevant statutes. As this study was not intended to be an exercise in the interpretation of statutes, but an analysis of the development and implementation of public policy in the field of secrecy and transparency in intelligence, I have not been drawn into a detailed review of the case law.

Lastly, it must be said that the research is exploratory. Premature conclusions and definitive conclusions on the basis of the data collected have been avoided, because the period in which access to information has been part of the political culture of South Africa has been relatively short. What the reader will observe is that the policy options or scenarios presented are, nevertheless, fairly extensive. I have taken the liberty of projecting a number of scenarios which even if they have not been experienced in a direct way by policy actors, may arise at some point in the future. This analysis is based partly on the experience of the intelligence services of other countries having to manage the tension of operating secretly in a democracy. This in my view is integral to the methodology of policy studies where all possible scenarios must be explored (Lee, 1991).

Underlying assumptions of the study

Democracy in South Africa has brought to the fore a number of concerns that affect the intelligence services as well as various other stakeholders within and outside of the state, each of which must confront choices around the appropriate balance between secrecy and transparency. These concerns were outlined in the first chapter, and include the following: What informs decisions about secrecy in intelligence? What dangers might lie in having too much (or too little) secrecy or transparency? What scrutiny and oversight should there be over secrecy measures? Finally, at what point in their life cycle can secrets be declassified? I have assumed these to be the critical questions for the reasons set out below.

First, in the international context – and this is evidenced through the literature on the relationship between secrecy, national security and good governance in countries around the world – fierce debates have raged around precisely these issues (Mathews, 1978; Turner, 1986; Lustgartern & Leigh, 1994; Robertson, 1999). The world over, excessive secrecy has bred unaccountable and abusive conduct by intelligence services. Following terror attacks on

targets in the USA on 11 September 2001 and on other countries since then, some governments have introduced legislation curtailing freedom of movement and access to information. This has sparked off debates about whether such restrictions are acceptable in a democracy, and the extent to which liberal values and principles must be compromised in the interests of national security (Todd & Bloch, 2003; Hauerwas & Lentricchia, 2003).

Second, the experience of South Africa prior to 1994 demonstrates that the secretive conditions under which the apartheid security and intelligence agencies functioned made possible the perpetration of gross human rights violations against anti-apartheid opponents. Thus, in the debates about the values that should underpin post-apartheid society, there was a widespread view among the participants at various for a, including the multi-party negotiations in the early 1990s that the balance between secrecy and transparency should be such as to ensure that similar abuses could not easily occur without detection (African National Congress, 1992; ISSUP, 1992). The questions which arose in those debate were around the role and rights of the public in ensuring accountability and transparency among public bodies, and how public bodies could be made to act in an accountable and transparent manner, the penalties for failing to do so, and the systems of checks and balances – inclusive of oversight structures - that should be established to ensure that public bodies upheld the principles of accountability and transparency. Even as I was gathering data, the question of how the records of apartheid security forces and their adversaries - the erstwhile liberation movements - should be treated so as to promote the goals of truth and national reconciliation in South Africa's transition to democracy, was as yet unresolved by government.

Third, a survey of academic writings from 1994 onwards, reflects that these have also been concerns of post-apartheid South Africa. Various analysts have expressed concern about the fact that the intelligence services, operating partly under an inherited regulatory framework, run the risk of acting unconstitutionally, if strict checks and balances are not implemented (Harris, 2002; Currie & Klaaren, 2002; McKinley, 2004).

The research process

In Chapter One, I made the observation that the post-apartheid intelligence services and critical policy actors have displayed some ambivalence about the extent of transparency that is appropriate. This state of affairs, I propose, calls for the development of guidelines that manage the tension inherent in protecting national security in a democracy, and upholding the fundamental right of access to information contained in South Africa's Constitution.

My interest in the development of policy aimed at improving the accountability of the security and intelligence services began in the early 1990s when, as an activist in the mass democratic movement in South Africa, I participated in research and debate on the future of the country's security forces. This involvement included participation in working groups directed at influencing the multi-party negotiations which resulted in the adoption of broad principles for inclusion in a future South African Constitution. The constitutional provision of a qualified right of access to information contained both in the Constitution of the Republic of South Africa Act, 1993 (or the Interim Constitution as it was widely known) and the Constitution of the Republic of South Africa Act, 1996, and the subsequent introduction of the Open Democracy Bill in 1998, suggested very strongly to me that there was need to develop a policy framework for the management of access to information generated or possessed by the intelligence services.

At the start of the research in 1999, I was the General Manager of the Intelligence Academy, the training facility shared by the National Intelligence Agency and the South African Secret Service. My position as a senior manager in the intelligence services made me all the more sensitive to the likelihood that it was only a matter of time before the services would be confronted with requests for access to records. I believed that in the absence of clear policy guidelines, the services' responses might prove to be inconsistent, unlawful, or even unconstitutional. Fortunately though, South Africa was not traversing entirely uncharted territory: a considerable body of English-language literature existed on how other countries

that promoted the principles of open government had found answers to questions concerned with the relationship between secrecy and national security (Mathews, 1978; Adler, 1991; Lustgarten & Leigh, 1994; Hazell, 1989).

The research process was iterative, and the questions begged repeated definition and refining. I had initially intended to devote considerable space to an analysis of the Open Democracy Bill. The bill eventually came into law whilst I was undertaking the research, by which time it had undergone several revisions as well as a change of title to The Promotion of Access to Information Act, 2000. Moreover, the Act has been subject to several legal interpretations, both through the courts, and by academics and non-governmental organisations. This has only served to enrich the body of resources available to me in my own research.

I went about the research conscious that there is a range of unspoken assumptions in the discourse of national security: these include the notion of threats to the interests of a homogenous state entity, whose citizens can be relied on for their loyalty to it, and who are tolerant of restrictions on their individual choices (Jones, 1995). The statements of policy-makers, bureaucrats and legislators were analysed with a view to unmasking the realities that lie beyond the discourse. A range of other primary sources contributed to this endeavour: interviews, legislation and court papers, all assessed with a view to understanding which classes of information in the post-1994 period, and especially since the passing of the Promotion of Access to Information Act of 2000, are subject to secrecy and confidentiality. I further explored which categories of information generated by the intelligence services are typically treated as unrestricted information, or are freely available to the public.

Next, the question of which officials in the intelligence services, and the state at large, have the authority to classify information at various levels of secrecy, and the legal force of such classification was examined, as was the question of how the records of the apartheid services - those that survived the mass destruction of documents in the early 1990s – are being preserved and managed. Other questions I posed to interviewees and tried to discern the answers to through my scrutiny of records concerned when and how, under the current

legislative and regulatory environment, a document lose its classified status, what the consequences for information thus disclosed, are. I also asked about compliance by the intelligence services with the requirements of the Promotion of Access to Information Act; and what role oversight bodies and civil society had played in shaping policy around secrecy and transparency.

The study took seven years to complete. When I began the research in 1999, the Open Democracy Bill had just been introduced in Parliament. The idea at the time was to assess the impact the Bill would have on the country's intelligence services, acting in a democracy where the right of access to information was upheld by the Constitution. The intelligence services, by law, were required to protect information relating to national security and this was a feature upheld by the Protection of Information Act, 1982. This made for a challenging policy conundrum, I believed, because clear criteria for exercising these options were lacking.

The passage of time, and the implementation of the Promotion of Access to Information Act, 2000, has made it possible for me to base my policy recommendations on concrete developments, including the intelligence services' levels of compliance with the Act, and several case studies where their interpretation of the Act has been demonstrated and put to the test. These developments have had to be analysed contextually: the democratic South African state has been faced in the first decade or so of its existence, with building credible institutions whilst delivering on its objectives, and has faced capacity challenges. In the case of the intelligence services these have related to the creation of the services, the establishment of oversight institutions and the role of organs of civil society.

The research tools

The very nature of my research domain – the intelligence services – is that it does not invite close scrutiny. Anticipating this reality, it was my own decision to avoid the use of secret or confidential sources of information. My strategy was deliberate; as one of the conditions for

gaining access to classified information, I might have had to subject myself to restrictions on the eventual dissemination of the dissertation, and I wanted to avoid this fate, believing that a subject such as secrecy needs to be debated in public. In any case, as I have already mentioned, I found that there was a significant amount of openly available material that had just not been subject to analysis, and that was a rich enough repository from which to compile my study.

I therefore conducted the research utilising unclassified information. There was a significant amount of academic literature available about the relationship between secrecy and democracy, and about the right of access to information. The main collections, reference and journal collections of the libraries of the University of the Witwatersrand, the University of Pretoria and the University of South Africa, were able to supply most of my secondary research requirements. Over the years, I also had access to the library collections of the National Intelligence Agency and the South African Secret Service, by virtue of my membership and position in the services.

Officials of the Department of Defence (DOD) provided me with unclassified and restricted policy documents, the "section 14" manual in force in the DOD, and copies of the court papers relating to the Southwood judgment, which I discuss in some detail in Chapter Seven. Copies of court papers relating to the SAHA challenge to the Department of Justice and Constitutional Development (DOJ) were obtained from that department. The SAHA also provided me access to their collections, thus improving my understanding of their concerns in this matter. Interviews also played a critical role in the data collection, as I was able to obtain through them, insight into the concerns of various stakeholders about the matters at hand.

The literature review

The role of the literature survey was critical, not only because it assisted in validating the research questions, but because it also provided a theoretical framework for interpreting the

data that was gathered in the course of the research. A review of the literature on the concepts of secrecy, national security and governance was conducted.

A review of the literature on security sector reform in Africa and South Africa was also undertaken. It was found that a significant number of analysts found that the process of redefining the post-apartheid security agenda was inclusive enough to guarantee, at least for the early (and current) years of democracy, reasonably professional security services with clearly defined mandates, in line with constitutional mandates that upheld a broad view of "human security" (Nathan, 1992; Cawthra & Luckham, 2003; Lala, 2004) Lastly, the literature on managing records in times of transition has been an important part of the study, suggesting a range of policy options from which policy makers in South Africa might learn (Hayner 2001; Posel and Simpson, 2002)

The research interviews

The research interviews were the primary source of data collection. At the outset of the research, I identified the following categories of potential interviewees:

- technical experts involved in drafting the Promotion of Access to Information Act;
- officials of the Department of Justice and Constitutional Development, which had the responsibility of ensuring the implementation of the Promotion of Access to Information Act;
- the head of the South African National Archives, concerning his institution's role as custodian of all state records, including the records in the keep of the security services;
- bodies provided for in the Constitution and national legislation to ensure transparency and accountability, including the Human Rights Commission and the Office of the Auditor-General;

- freedom of information advocacy groups such as the South African History Archive Trust, on their experience of gaining access to information held by the state; and
- officials of the intelligence departments whose mandates included promoting national security, on their implementation of the access to information requirements of the constitution and national legislation.

From July to October 2003, I was granted a sabbatical by my employers to conduct field research. It was during this time that most of the interviews were conducted, and an intensive revisiting of the research problem sharpened my conceptualisation of it. In a second period of sabbatical leave, from June to September 2005, I conducted further interviews.

I was able to access policymakers and persons involved in the formation of the intelligence services, the drafting of legislation that would impact on the services, and decision-makers in the oversight community of South Africa, without much difficulty. Prior to each interview, I prepared structured interviews for each of the respondents and circulated them in advance, to give them time to prepare. The average duration of the interviews was one hour and thirty minutes. During the interviews, I made written notes of the responses, which I then transcribed, and later analysed so as to incorporate relevant responses into my study. In some cases, as I developed an aspect of research or branched into further areas of enquiry, a second interview became necessary, but this was generally not the case.

The case studies

According to Yin (2003), the case study is a favoured research strategy in a wide-range of disciplines, including the traditional fields of sociology, political science, anthropology, history and economics, as well as the practice-oriented fields of urban planning, public administration, public policy, management sciences and education. Case studies are useful in illuminating why decisions are taken, and this is appropriate in the context of this study. Moreover, according to Yin (2003), case studies are useful because, as empirical studies they lend themselves to investigating contemporary phenomena within their real-life contexts, and use multiple sources of evidence.

Analysis of several cases studies illustrating how the Promotion of Access to Information Act, 2000 has been interpreted by government departments, where national security was of concern, was particularly insightful. Even though there have been relatively few examples where the intelligence services have been challenged in the courts for their decisions around the application of the legislation, important legal arguments concerning classified information have been tabulated, and a few relevant judgments have been given in the courts; some of these are reviewed in the study. One example was the application by SAHA for access to 34 boxes of files of TRC records, which it believed were unreasonably being withheld by the intelligence services. The 34 boxes contained records which had been deemed "sensitive" by the Chief Executive Officer of the TRC, and handed to the Minister of Justice, who at the time of receiving them in 1999, was also the also minister responsible for the intelligence services. The study explored the postures of the various role players on the question of access to the information contained in the 34 boxes. I analysed the reasons given by the Minister of Justice for withholding the records, and how they were handled in the period they were under contestation. I compare and contrast this with the criteria used by the state to assess another request by the SAHA for access to certain records of the SANDF, in order to assess differences or similarities in the criteria used by different departments for access to apartheid-era records.

Interpretation of the research results

Interpreting the literature

The review of the literature was an ongoing part of the process and revealed many relevant viewpoints: about the definition of national security; about the tensions of secrecy in a democracy, and about the challenges of security sector reform. The literature was also useful in unearthing the roots of governmental secrecy and the emergence of the post-apartheid intelligence dispensation. The extensive review of secondary resources, coupled with primary research, particularly in-depth interviews, provided a richly textured account of the reality of balancing secrecy and transparency, against the background of national security concerns in

South Africa. The comparative analysis has been an equally important dimension and the study of how intelligence service records have been managed in various democracies, as well as in societies undergoing transition, has been most instructive. I was able to draw on the recurrent trends and principles that emerged in the various country studies, in my formulation of policy recommendations in Chapter Eight.

Interpreting the interviews

Because I interviewed a wide range of role players, I had anticipated wide disparities in their positions. However, there was remarkable convergence in the views. For example, there was general acceptance by all the role players, that whilst the aims of the legislation were laudable, the capacity for implementation was poor. I have factored these similarities in viewpoints, as well as the differences that may exist, in my formulation of policy recommendations, in order to make them as relevant as possible. In spite of the restrictions on disclosure about the intelligence services, my position of trust afforded me access to informed and influential stakeholders within the intelligence services, allowing me to access to the views of those I most needed to assess.

I therefore considered the interview results, which I understood to be inherently subjective, along with other research material, including the legislation, discussion documents, court affidavits and judgments, official reports of the Joint Standing Committee for Intelligence and the Auditor General, and assessments undertaken by legal and policy experts.

There were some deficiencies in the interview process. I did not, for example, interview all possible sources of information. Given that I placed much store in the examples of other countries, interviewing foreign government representatives of the US, Canadian and Indian intelligence services, based in South Africa would have been ideal, and might have resulted in deeper insight. On the whole though, I considered the interviews successful in helping me to achieve the research aims.

Interpreting the case studies

My main point of reference for the case studies was the court papers filed by respondents and applicants and where available, the judgment of the court. This was supplemented by the interviews, the literature on the South African experience and also the comparative studies. Against the background of the preceding chapters, I presented the views for and against disclosure that the respective parties had put forward. Based on my own assessment of the principles, I provided a critique of their positions. I was able to do this because the in-depth literature review, the study of the legislation and the Constitutions, the comparative review with other countries, had provided the material with which to make a reasonable assessment.

Concluding remarks

The study of policy around managing access to intelligence information in post-apartheid South Africa is essentially a qualitative study, concerned with the development of appropriate norms for balancing secrecy and transparency in a democracy. The views and assessments of policy stakeholders have therefore been a critical component of the study, and I have presented the perspectives of the most significant players, in order to state my case. These views have been presented against the background of the context in which the constitutional state of a right of access to information in South Africa has arisen, as well as a vast international experience of attempting to balance national security imperatives and the rights of citizens in a democracy.

CHAPTER THREE

LITERATURE REVIEW

Introduction

This chapter examines some of the literature relevant to a study of managing access to intelligence information in a democracy. These include, firstly, a conceptual treatment of the benefits and pitfalls of secrecy in a democratic society. I also explore the literature on balancing secrecy and transparency in international relations, with emphasis on critiques of instruments established by international and regional bodies to regulate or provide guidelines in this arena. The review also examines trends in the concept of national security and the democratic control and governance of security institutions, first in the Western literature, and then from the perspective of the developing world, particularly Africa. This is important because the policy debate around secrecy and transparency is only one of a general set of policy concerns that have seized analysts of national security in the developing world. The literature therefore explores the general themes of this debate in order to assess their relevance for South Africa. I do this, having focused on the literature on secrecy and transparency in the context of the new South African Constitution, but also the literature on managing security records and the politics of memory in societies undergoing democratic transitions is another area that informs this study.

Conceptual approaches to secrecy

Bok (1982) tackles the concept of secrecy from an ethical and philosophical standpoint, before exploring its application by the state machinery. She attempts a "neutral" definition of secrecy, describing it as "intentional concealment", involving the deliberate withholding, hiding or concealing of information in order to prevent someone else from uncovering the

shielded information. Refusing to accept all secrecy as inherently immoral, Bok describes some of the social contexts in which secrecy might arise or be applied, including among these medical research and practice, secret societies, trade negotiations, research, and the protection of military or state secrets. Secrecy is portrayed by Bok as utilitarian and justifiable in many cases. Often moral and ethical judgements are required about the consequences of secrecy. She attempts to answer the question of when secrecy can be considered acceptable, by suggesting that the moral arguments for any secret practices must be able to stand the test of public debate. Moreover, the criteria for secrecy should never require concealment. A means test she proposes for whether secrecy is acceptable or not, is that the reasons for the secrecy should be capable of being argued convincingly in public. In this regard, Bok (1982) is particularly suspicious of state secrecy and argues in favour of severely limiting the use of secrecy by the state, because of its association with power.

Her work on secrecy follows an earlier analysis of lying and deception (Bok, 1978). In this work, Bok had attempted to demonstrate that lies and deception could arise or be applied in a number of social contexts, and that their impact had to be assessed in context. Among the contexts for lying were the following: white lies (usually considered harmless); lying to enemies (as tactically applied in a state of war); deceptive methods of social science research; paternalistic lies (concealing an unpleasant truth from a child, for example or deception of the terminally ill about the state of their health). She argues that careful consideration should be given to the consequences of truthfulness or deception, whenever such a choice has to be made, but accepts that serious dilemmas may arise. She urges that an orderly social system is dependant on a reasonable degree of truthfulness, and suggests that the truth should not be unduly subverted.

The social costs of lying, Bok (1978) warns, include a disproportionate allocation of power to groups disempowered due to their lack of access to reliable and cogent information, and the consequent inability of those so affected to exercise appropriate choices in favour of physical survival. In addition, there is the psychological and emotional burden of uncertainty to be carried by those who are the victims of lies.

Bok's works (1978, 1982) have relevance for the intelligence services of post-apartheid South Africa, because they prompt us to confront the complexity and consequences of secrecy and confidentiality. The case of the intelligence services is especially challenging, not only because of the professional duty of secrecy (enjoined for example, by the relationship between secret human sources of information and the services, or the confidential nature of intelligence liaison between states), but because such secrecy is specifically provided for in law, its breach carrying the burden of criminal sanction.

Robertson (1999), writing on the policy question of secrecy in the British state, has conducted a critique of Bok's work on secrecy. He is critical of Bok (1982) for providing no convincing criteria by which to judge when secrecy has become excessive, and claims that this diverts from her stated desire for a neutral approach to secrecy when addressing the role of the state; in other words she all but condemns the state for having ignoble intentions in the pursuit of secrecy. According to Robertson (1999:12):

> The main thrust of Bok's analysis is that secrecy is particularly dangerous when those who employ it are holders of power for, in the absence of accountability and safeguards, secrecy makes such people even more powerful. The balance of the moral argument has dramatically switched so that what was seen as a mechanism of defence, protecting the integrity of the personality, is now a weapon of offence, associated with the aggrandisement of power.

Robertson's (1999) objection to Bok's (1982) assumption that secrecy in government is generally bad for society is relevant to our study. The intelligence services in a democracy – at least in South Africa – are required by law to conduct their operations in secrecy. Where there are checks and balances on their powers, as exercised through oversight mechanisms, it appears to be simplistic to conclude that they will abuse their powers, or even that there are no valid reasons and benefits to their functioning in this way. It

is unfortunate that Bok (1982) who so competently made the case for secrecy in other spheres of life was not able to provide a more balanced account of its usefulness when exercised by the state.

But Robertson (1999) was not so much concerned with secrecy, as with the role and relevance of "freedom of information" in democratic political systems. He is in fact, critical and cynical about freedom of information or "access to information" as it is otherwise referred to, as a vehicle for open government. For Robertson (1999), the introduction of freedom of information legislation in many countries has been in response to crises precipitated by governmental excesses, and serves to streamline the channels of communication between the public and the state. If, as he contends, information constitutes itself as a form of power, then the management of information may well serve the ultimate end of providing political leverage to those who are in power.

Robertson (1999) argues that the methods by which governments exercise control have changed the balance of power between different groups within the British state. This has called for new strategies of information management, including a changed relationship between elected politicians and bureaucrats. One example of the change is that elected politicians are held to account with greater vigour by their constituencies, than in the past. It therefore now serves the interests of Britain's ruling elite to place the onus on the public to request access to information.

For Robertson (1999) the most contentious aspect of access to information legislation is who the beneficiaries of the transparency are. Robertson is begrudging in his assessment of the benefits of freedom of information legislation. In the first place, in his view it does not easily allow people to access information about critical information about policy-making. Rather, it allows readier access to personal files.

However, Robertson concedes (1999:158):

> It help ensure that records are more accurate, which is of benefit to governments; and fairer, which is of benefit to citizens. The problems arise when this modest but worthwhile reform is confused with open government. FOI is not an important part of creating more open government, making the process of political decision-making more transparent and more open to citizen participation. There are quite other mechanisms that do this. The creation of a more federal structure, with competing centres of decision-making, is far more important to this process.

This analysis is pertinent, because it cautions us against regarding access to information as the only measure of accountable and open government in the South African situation. Indeed, along with entrenching the right of access to information, the RSA Constitution institutionalises a range of measures and instruments to facilitate open and accountable governance. These include the separation of powers between the legislature, Executive and the judiciary, the establishment of oversight committees in Parliament, and the independent auditing of the financial statements of all government departments (RSA Constitution Act, 1996). Any assessment of accountability of the intelligence services must therefore take into account how these institutional measures are applied in relation to them.

Balancing secrecy and access to information in international relations

There has also been academic commentary on access to information in the international regulatory domain that is of relevance to this study. Access to information is recognised as a basic human right in several international covenants. However, international law permits governments to legislate in favour of the protection of state secrets (D'Souza, 1999).

Reference can be made to several international covenants, which whilst promoting freedom of information, subject this right to qualifications. Evatt (1999) points to the International Covenant on Civil and Political Rights (ICCPR), adopted by the United Nations (UN) in 1966, and entered into force in 1976. In terms of Article 19 of the ICCPR, freedom of opinion and expression are guaranteed, but are subject to restrictions, including the protection of national security or of public order.

Evatt (1999) points out that some guidelines for ensuring the compatibility between individual states' legislative regimes and the ICCPR are available, but that it is up to the state to show the legal basis for any restrictions imposed on the right to freedom of expression. In assessing an instrument such as the Covenant, one has to assess what impact it has had on governance in individual jurisdictions. It would appear that its effects have been minimal in real terms, at least in the area of freedom of expression. At best the Human Rights Committee of the United Nations has been able to highlight individual states' deficiencies, but these interventions do not translate into punitive measures for a state where there are digressions (Evatt, 1999).

Like the UN, the European Union (EU) represents another example of a supranational authority, whose instruments are binding on all member states. In general terms, European law is gradually encroaching on national law, which in most cases maintains precedence. Whilst the EU is said to be founded on four freedoms (of movement of persons, capital, goods and services) each interest may be curtailed in the interest of national security Moreover, Nichols (1999) informs us, in terms of the Treaty of the European Union, no member state is obliged to supply information if such disclosure can be considered to be contrary to the essential interests of its security. Also, any member state of the European Union may take such measures as it considers necessary for the protection of the essential interests of its security, particularly in connection with the production of, or trade in, arms, munitions and war material.

The EU has made strides in defining the categories of information that must be made publicly available, including information from private sector companies, and information held by public authorities about the environment. Member states are not obliged to disclose information regarding international relations, national defence and public security. Moreover, The EU directive requires member states to allow a person who considers that his or her request for information has been unreasonably refused or ignored or has been inadequately answered by a public authority, to seek a judicial or administrative review of the decision in accordance with the relevant national legal system (Nichols, 1999).

The right of access to information has also featured in African instruments of cooperative governance. The African Charter on Human and People's Rights (African Charter) was accepted by the majority of members of the Organisation of African Unity (OAU) during its existence, but like the ICCPR, had limited impact. Somewhat overwhelmed by the realities of political life in post-colonial Africa the OAU's African Commission of Human and People's Rights was responsible for the supervision of the Charter which dealt with access to information in Chapter 9, which stipulates that every individual shall have the right to receive information, and that every person shall have the right to express and disseminate his opinion within the law.

Nevertheless, it is clear that secrecy is recognised as having a legitimate role in the international political system. Intelligence is therefore seen by states as being as relevant as ever, if not more so today than previously. In an increasingly uncertain world, even multilateral institutions such as the United Nations are considering the role of intelligence: this is a challenge for an organisation such as the UN given that the world body is devoted to transparency. Increasingly in its peacekeeping role, and for the security of its own humanitarian operations, the UN through experience seems to be coming to the conclusion that it does after all, require an intelligence capacity. Dorn (1999) makes a strong argument for UN secrecy, where the success of a UN peacekeeping operation (PKO) may depend on secrecy and early warning gained through intelligence gathering. He argues further:

> Secret intelligence is even more important in modern multidimensional PKO's with their expanded responsibilities: elections monitoring, where individual votes must be kept secret; arms control verification, including possible surprise inspections at unannounced locations, law enforcement agency supervision (to 'watch the watchmen'); mediation where confidential bargaining positions that are confidentially shared by one party with the UN should not be revealed to the other; sanctions and border monitoring, where clandestine activities (e.g. arms shipments) must be uncovered or intercepted without allowing smugglers to take evasive action.
>
> Dorn (1999:3)

Dorn (1999) is concerned that the UN does not have any guidelines to deal with sensitive information, and that the variances in individual PKOs' information management systems undermine the effectiveness of the institution. He urges that the UN needs to acquire the means to make effective use of both open and secret information. As with any intelligence system, standards should be set for determining what information should be gathered and held openly, and what should be gathered and held in secrecy, and for what duration. He offers the guidelines that information should be open unless divulging it would result in death or injury to individuals, bring about failure of a UN mission or mandate, violate the right to privacy of one or more individuals, or compromise confidential sources or methods.

These arguments demonstrate that the concerns that the UN must face about the role of intelligence in its system, are little different to those that many countries, including South Africa, currently face. These potentially are also the issues that face other multilateral institutions, such as the Southern African Development Community (SADC) and the African Union (AU). The challenge in relation to both these bodies is managing common security objectives in a global context where competition is a reality. SADC is not an extensively polarized bloc, and prospects for regional integration, peace and security may be thought to be considerable, but only if one looks at these matters narrowly. If a human security perspective is adopted, then the many problems of economic, food and environmental security pose challenges.

Moreover, problems of transnational crime are a clear basis for inter-state cooperation. Malan & Cilliers (1997) point out that SADC has an elaborate organizational framework purportedly geared to addressing the region's security challenges, but that problems of capacity and alignment need to be addressed if the structures, including the Inter-state Defence and Security Committee (ISDSC) which provides for the sharing of intelligence, are to be effective. Possibly the biggest threat to intelligence cooperation is the lack of resources on the part of most of the governments in the region.

In summary, the literature demonstrates that the right of access to information is strongly established in various international instruments. This does leave the impression that the case for secrecy, in the post-apartheid dispensation may well have been neglected. Justifiably, out of concern for a repeat of the excesses of the past, there has been much attention paid to the right of access to information in academic analysis. However, it may well be time for a body of responsible analysis that puts forward, against a realistic assessment of threats to security, a compelling case for confidentiality and secrecy. It is out of such countervailing analyses that a balanced policy analysis and options may emerge.

Secrecy and transparency in liberal democracies

The South African intelligence services, like their counterparts in many parliamentary democracies, conduct much of their work - aimed at promoting national security - under conditions of secrecy. In the Western literature, it is often assumed that there is a causal link between governmental secrecy and the abuse of power. It is also suggested that there is an implicit tendency towards fair and judicious government when greater public access to information, particularly about the security and intelligence services of a country, is the order of the day (Halperin & Hoffman, 1977; Richelson, 1989; Steele, 2001; Hodess, 2003). In South Africa there is an increasing public expectation that more information about the security and intelligence services will be made available to the public, and that these bodies

will be held accountable for their actions, past and present (Africa, 1992; Nhlanhla, 1992; Harris, 2000; Bell, 2001; Klaaren, 2002; Levy, 2004).

In the literature on the relationship between secrecy and transparency in a democracy, we also encounter several analyses of the social and political costs and benefits of these policy imperatives (Franck & Weisband, 1974; Turner, 1986; Shulsky, 1991; Halperin & Hoffman 1977). Some of the studies derive from the authors' involvement in the security communities of their countries, and take as a given, the role of espionage in international *realpolitik*. Franck & Weisband (1974) point out that the delicate balance between the government's need for secrecy and the people's right to know has been the subject of intense academic and public concern in many western democracies.

The contradiction in managing the conflict between the secrecy required by intelligence activities and the normal openness of democratic societies for example, is addressed by Turner (1986), who points out that the reason the US government introduced measures to counterbalance secrecy with transparency measures in the seventies and eighties, was their experiences of unacceptable conduct within their security services, especially the intelligence community.

Some writers have argued that a lack of openness has had the effect of fuelling suspicion and a public belief that the secret services have hidden and subversive agendas (Aubrey, 1981; Cohen, 1982; Mates, 1989). The dilemma for the intelligence services of a democratic state is that such an analysis, carried to an extreme, may demonise them unfairly, and fail to recognise the role that they could play in providing early warning about threats to the security of a country and its people (Todd & Bloch, 2003). In addition, there is debate in democratic societies on the extent to which states should institute secrecy measures. Steele (2001) has argued that much intelligence and early warning about security threats can be gleaned from openly available sources of information.

Mathews (1978) points out that theoretical writings on liberal democracy have long supported the notion that the right to know about the actions and decisions of the executive and its administration are essential elements. In Western democracy, he argues, there have been variations on this theme; for example, in British politics, "Tory democracy" has propagated the view that the masses have a duty to obey their elected leaders (Mathews, 1978). Mathews cautions that this elitist concept of democracy fails to analyse the problem of alienation from democratic government in mass societies. He argues that extensive secrecy in the Executive branch and its departments is incompatible with democracy.

Beside the alienation of the masses from the Executive, Mathews (1978:14) points to the growing might of bureaucracy as a general phenomenon in Western political systems:

> The bureaucracies, it is now clear, have become centres of power in all Western democracies, including those that have presidential type executives. Viewed from the perspective of access to information, this is an alarming development since official secrets were the invention of the bureaucracy. Secrecy has been, and remains, one of the most effective techniques which officials have employed to enhance their power.

The consequences of official secrecy are the creation of a climate of distrust between government and its officials on the one hand, and the citizens of a country on the other. People tend to believe less and less of what government says because they feel they do not have access to corroborating information. A perception of government misinforming them sets in, even where this is not the case, whilst government becomes increasingly frustrated by the simplistic analyses of the public whose opposition is perceived to be motivated by misunderstanding and simplistic and extreme responses (Mathews, 1978). Mathews's analysis is pertinent to our study of access to intelligence information. Perhaps more markedly than any other department of state, the South African intelligence services routinely withhold information from the public, and even from other government departments. As a result, little is known about their functions, both by the public and to an extent, some within the

Executive. The problem of intelligence services' alienation is one of the most significant challenges that the post-apartheid South African state must overcome.

Secrecy and transparency in societies in transition

How countries whose security and intelligence services are subject to access to information legislation, manage in practice their responses to requests for disclosure about the activities or conduct of their intelligence service, is often fraught with contradictions (Rankin, 1986; Hazell, 1989; Leigh, 1997; Coliver et al.,1999). Banisar (2002) cautions that the mere existence of access to information legislation does not always mean that access is guaranteed in a particular country. In many countries, enforcement mechanisms are weak and very often, governments resist releasing information. Alternatively, bureaucrats delay the processing of information requests.

The literature on the tensions between secrecy and transparency in societies undergoing transitions may also hold some use value for this study. Several English-language studies, written by Western analysts, have sought to uncover the inner workings of the former eastern European intelligence services, using records disclosed in the period following the Cold War (Childs & Popplewell, 1996; Williams & Deletant, 2001). The declassification of records in the USA has played a significant role in revelations about the role of the Central Intelligence Agency (CIA) in many post-conflict scenarios around the world. Hayner (2001) writes about the difficulties truth commissions often encounter in accessing official records of former repressive regimes. However, some states undergoing transitions have been able to fill the information gap by accessing declassified records of other states.

Particularly in the case of the Salvadoran and Guatemalan truth commissions, extensive use was made of records declassified in terms of the US Freedom of Information Act. These Commissions made use of non-governmental organisations such as the National Security Archive that had experience in declassification procedures (Hayner, 2001). The Salvadoran

Commission, for example, relied on the files of already declassified documents, but also applied for the declassification of additional documents. Although it initially met resistance from some departments of the U.S. government, cooperation improved with the inauguration of President Bill Clinton in January 1993. The Guatemalan Commission made much more extensive use of United States documentation, and through the National Security Archives, submitted freedom of information requests on over three dozen cases they were investigating. The release of the information and the use of declassified records played an invaluable role in explaining the United States government's relations with the above-mentioned states, and providing insight into the role of the US intelligence services in the 1960s and 1970s.

This factor - access to declassified records of former, authoritarian regimes - is of relevance in view of the apartheid experience of the destruction of intelligence records, and the ambivalent relationship between the State Archives and the intelligence services. As revealed through the hearings of the Truth and Reconciliation Commission (TRC) - initiated through a law of parliament to uncover gross human rights violations that had been committed during the apartheid period - accountability for the preservation of official records is at the heart of preserving national memory, and may play an essential role in bringing closure to traumatic episodes in the lives of previously divided nations. The South African experience of managing official files from the apartheid era contrasts sharply with the case of several former eastern European countries where files of the former security services were thrown open to the public for scrutiny, following the collapse of communist regimes. The argument in the case of the eastern European post-communist authorities was that disclosure was a necessary, if painful, exercise in coming to terms with the past. These contrasting experiences lead us to consider the role of the archive, and the process of recording and documenting history, as a fundamental prelude to accessing information.

Hamilton, et al. (2002), question the traditional conception and role of state archives. They warns that state archives can falsely construct the past through the control of selection, description and access to information. As a consequence, historians have been cautious about relying exclusively on public and more specifically government records, because of their colonial and later apartheid biases.

Petersen (2002) stresses the need therefore to,

> …occupy ourselves with locating, understanding and foregrounding the various forms of oppositional experiences and knowledge systems that are currently omitted from the archives in their present figuration….In short, without a subtle grasp of the forms, contents and intentions of seemingly 'informal' canons or archives, any remaking of the archives is bound to be informed by the assumptions of the official processes and discourses.
>
> Petersen (2002:30)

What Petersen is reflecting is that archives are really just a reflection of how states want history to be recorded. State archives also reinforce the isolation and secrecy of information: once buried in the archive the record in a way, no longer exists, except for those who are its immediate custodians, and others who might develop some arcane interest in it (Petersen, 2002).

Hayner (2001) also argues for an alternative approach to the management of official records, particularly in transitions from authoritarian to democratic rule. She notes the increasing body of literature on transitional justice, of which her own work may be considered a part. In her words, these studies are

> …a subset of the broader field of inquiry into democratic transition. The basic question, that of how to reckon with massive state crimes and abuses (or abuses by groups in opposition to the state), raises a wide range of legal, political and even psychological questions. This field - to the degree that it has taken shape as a defined field unto itself - has developed in response to the demands and differing circumstances of many transitional states around the world, and

> the increased public and international expectation that accountability is due after atrocity.
>
> Hayner (2001:11)

The measures of redress that may be chosen by states in the aftermath of periods of atrocity includes the prosecution of perpetrators through the courts (although the success of such a trial may be mediated and diluted by the political compromises that the transitions have entailed); international tribunals (an option with the limitation lying in the number of persons who can in reality be brought to account by such bodies, relative to the actual number of perpetrators); the removal or barring of persons from public office (a practice common in the former Eastern European states); or targeting members who had been part of the repressive security forces and barring them from participation in the post conflict security forces. Lastly, access to the files held by the former security forces was a measure favoured by some former communist countries following the end of the Cold War. Another form of redress has been the initiation of inquiries into widespread abuses by state forces.

Hayner (2001) has studied at least 21 such processes that have taken place since 1974. Generically referred to as "truth commissions", they include "commissions of the disappeared" in Argentina, Uganda and Sri Lanka, "truth and justice commissions" in Haiti and Ecuador, a "historical clarification commission" in Guatemala, and "truth and reconciliation commissions" in Chile and South Africa. These truth commissions, while they may have different emphases, compositions, mandates and resources, share the following characteristics: they focus on the past; they investigate patterns of abuses over a period of time; they operate within a defined time frame, usually less than two years; and they are officially established and empowered by the state, often as a result of a negotiated political settlement or peace accord.

Their official status is also important because this gives them better access to official sources of information, increased security to undertake sensitive investigations and a greater likelihood that their reports and recommendations will receive serious attention from the authorities, which in the first place had commissioned them. Hayner's study (2001) points out several challenges faced by truth commissions, including problems of resources and language barriers, raised expectations, resistance by officials of the outgoing regime, and a lack of

access to official records. In many cases records may have been destroyed by members of the outgoing regime. This was precisely the problem encountered by the Truth and Reconciliation Commission in South Africa. Posel & Simpson (2002) contextualise how contested the South African truth commission process was. They explore the mandate, methodology, legal and political context and resource constraints faced in the process. Cherry, Daniel & Fullard (2002) elaborate on the challenges faced the TRC, including its wide-ranging mandate, difficulties in reaching consensus on the appropriate balance of methodologies, developing appropriate language or discursive paradigms with which to address or problematise sensitive issues, the weighting to be attached to the role of historians as opposed to lawyers, and organisational problems of time, space and the management of the vast records accumulated during the process.

In the case of the last-mentioned challenge, Cherry, Daniel & Fullard (2002) observe with regret that that the pressures of time and the need to maintain a narrow focus did not permit a more detailed examination of state records during the TRC. As the Commission was concerned purely with gross human rights violations, it focused on accessing documents directly relevant to this brief, in particular records about the apartheid state's security policies and structures. Ideally, they argue, a dedicated team of archival researchers should have been created to study all documents so as to gain a fuller appreciation of how the apartheid state had functioned.

Pigou (2002) recounts the difficulties in gaining access to official information that were encountered by the investigation unit of the TRC, and claims that the security forces including the SAPS, the SANDF and the NIA, to varying degrees, blocked access to the records of their predecessors. Simpson (2002) argues that it is important to understand both the strengths and weaknesses of the truth and reconciliation process in South Africa, and to recognise it for its unique qualities, including the nature of the negotiated political settlement out of which it was wrought.

These perspectives on the archive, and accessing official records during the transition, are relevant to the debate on secrecy and access to information generated in the context of national security imperatives. A lesson from this debate on state archives is that we should be

careful not to mistake the state's record or version of reality, as the final reflection of truth. A range of non-state actors may well view the same phenomena through entirely different lenses, and this does not make their reflections less important or valid. It is therefore important that the process of documenting these different realities are taken into account when appraising any past reality, and that the state's official policy on national security be appropriately formulated, rather than continue to marginalise less powerful groups in society .

The second lesson arising out of this debate is the need to seriously reconsider how to promote accessibility of state records and archives, and to avoid the perils of undermining public ownership of a country's history. Apart from marginalising significant voices in the South African arena, the State Archives Service under apartheid did not intervene when state structures went about destroying official history. The need to preserve history, unaltered and representative, is therefore another lesson from our past. How these lessons are to be applied in the context of state structures which exist, almost literally in the shadows, is a huge challenge. This study has yet to deconstruct the implications of access to information about or from the intelligence services. Presumably, any information which falls outside the scope of one of the Act's grounds for refusal of access to information may be requested and potentially answered.

Practical choices have to be made by the public and by the intelligence services and other public bodies regarding their relationship to information. Important intermediaries are to be found in the policy-making and governance communities, and in non-state actors. As in my discussion on the philosophical dimensions of secrecy, and the practice of securitization, it seems that once again the underlying power relations underscore the choices that are made.

Cawthra & Luckham (2003) argue the need to take into account the multi-faceted nature and complexities of the struggles for security in current day transitions from authoritarianism. In the first place such transitions do not always have democratisation as an ultimate end product or goal. Very often they result in protracted instability, or the replacement of one form of patrimonialism with another. Thus,

> ….instead of seeing the security sector as a coherent and unified 'sector', it may be more fruitful to see it as a shifting terrain of security coalitions, which are assembled and reassembled as crises occur.
>
> Cawthra & Luckham (2003:17).

It may be a fatal flaw to ignore the details of transition processes, including the actors involved and the interests they represent, the nature of the conflict and the role of intervening forces, and even historical factors. Cawthra & Luckham (2003) argue, further, that even democratic governments may use their security forces simply to consolidate their positions of power, and that war often becomes a significant economic driver and a manifestation of a contest over resources and wealth opportunities. In their words, because military governance in the post-Cold War era has been 'deligitimised',

> a different *kind* of analysis is required from that found in the more traditional civil-military relations literature. This would focus on a range of new issues, including the diverse and often subterranean forms of military political influence under civilian or democratic regimes; the role of other security apparatuses, including the police and intelligence services; the privatisation of violence and emergence of non-state armed formations; the spread of armed conflict and its impact on security including human security; and the complex and troubled relationship of all of these with democratic governance.
>
> Cawthra & Luckham (2003:10)

The authors are optimistic about the South African transition, which Cawthra (2003) describes as having had features that are promising of an enduring democracy. The implication of the issues they raise, is whether the intelligence services are as transparent and accountable as they need to be to avoid the risk of becoming authoritarian. The instruments of policy-making would have to be how inclusive of public debate, to mitigate this risk. Also strong oversight mechanisms would have to be in place.

Secrecy and transparency in South Africa

There is significant legal precedence in South Africa around access to information and the disclosure of information in various contexts other than the intelligence services, some of it pre-dating the new Constitution. Some analyses centre on discussing the right of access to police dockets or records by a defendant in a criminal matter: they include those of Bursey (1990), Cassim (1996), Jazbhay (1997, 1998, and 2002), Meintjies-van der Walt (1995), and De Villiers (2003). The following writers have explored the question of access to information concerning environmental rights: Glazewski (1994), Du Plessis (1998, 1999), Kidd (1999) and Grinlinton (1999). Concerning access to medical records, studies include those undertaken by Van Wyk (1996), Driver-Jowet (1998), Van der Poel (1998), Strauss (1998), Van Oosten (2000), Gaum (2001) and Blackbeard (2002) whilst Deale (1994), Landman (1996), Grogan (1997) and Le Roux (2001) cover the subject of access to information in labour relations. Finally, the following writers have commented on access to corporate information: Malan (1989), Solomon (1995), Carnelley (1999), Pimstone (1999), Matlala (2003) and Schulze (2004).

The introduction of a Bill of Rights, both in the RSA Constitution Act, 1993 (the Interim Constitution) and the RSA Constitution Act, 1996 (the Constitution) was the basis for several more general analyses of the right of access to information in South Africa. Some writers on the subject included Mureinik (1994), De Villiers (1995), De Vos (1995), Burns (1997), Currie (1999, 2000) and Wessels (2002). The introduction of the Open Democracy Bill in 1998 and the passing of the Promotion of Access to Information Act in 2000 were the basis for the commentaries of Govender (1995), Roos (1998), and Visser (2002). All the above writers have considered the implications for the policy and judicial landscape of the introduction of a constitutional right of access to information.

The most comprehensive and authoritative recent legal study of South Africa's Promotion of Access to Information Act, 2000 is a study undertaken by Currie & Klaaren (2002). The authors describe the drafting history of the Act and its interpretation, impact and application.

They also cover the mechanisms for the processing of requests and analyses in detail, the grounds for refusal of access to information as provided for in the Act. The authors discuss the relationship between the Act and the constitutional right of access to information, pointing out that the Act has a constitutional status, which should not ordinarily be capable of being undermined by Parliament. They argue further that:

> In the absence of an express provision, the usual rule of statutory interpretation is that earlier legislation that is inconsistent with subsequent legislation with the same or a higher status is impliedly repealed by the latter. Currie & Klaaren (2002:30)

This rule of interpretation is the basis for concern about the continuing application of the Protection of Information Act, 1982, even after the passing of the Promotion of Access to Information Act. Currie & Klaaren (2002) are concerned that the disclosure of the information through any means other than in response to a formal access to information request remains subject to law and regulations preserving confidentiality in government.

A central theme in modern analyses of governmental secrecy in South Africa is that they are located in a time and framework of deep concern about the excesses of South Africa's apartheid reality, which saw secrecy being used to cover governmental excesses (Mathews, 1978; Currie & Klaaren, 2002; Levy, 2004; Qunta, 2004; Steytler, 2004). There is a preponderant concern in the work of writers of the post-1994 period that society should not revert to that dark past. An unintended consequence of this concern may well be that, whilst the case for transparency is compellingly made, the case for legitimate secrecy may be neglected.

Levy (2004) has grappled with the challenges of managing the tensions between the public's right of access to information and the intelligence services' right to withhold information. He points out that the existence of the services is a constitutional requirement, and that they have

a duty to preserve secrecy, and to protect from disclosure, sensitive information in their possession. Qunta (2004) points to legal precedence, both locally and internationally, which holds up the principle of protecting the identities of sources, at least in police investigations. Zulu (2004) however, reminds us of the consequences of the Executive not being in a position to review the credibility and reliability of information, pointing to the politically costly decision of the USA and the UK to go to war against Iraq.

Steytler (2004) also recognises that the intelligence services in South Africa are faced with the challenge of balancing the requirements of the Constitution, with their legally defined role and methods permitted in law. He explores the strengths and weaknesses of particular vehicles for investigating matters concerning the intelligence services, listing these vehicles as internal investigations, and investigations undertaken by the Inspector-General for Intelligence, the Joint Standing Committee on Intelligence, the Public Protector, and Commissions of Inquiry. Steytler (2004) is optimistic that leveraging the right vehicles, possibly in combination with each other, can yield a result that upholds the principle of access to information.

There is at least one vacuum in the literature: very little analysis has been devoted to the study of the implications of access to information legislation and the constitutional right of access to information, for the South African intelligence services. Klaaren (2002) has been pioneering in this respect, and has expressed what he considers to be a fundamental concern, namely that the right of access to information is undermined by the continued existence of the Protection of Information Act, 1982. Moreover, he argues, certain instruments imposing administrative secrecy in government are based on legally unsound and possibly unconstitutional arguments. In this regard, Klaaren has taken issue with the Minimum Information Security Standards (MISS), a Cabinet directive providing criteria for the withholding of security related information from the public. Klaaren argues that the spirit of the MISS and in particular its security screening procedures contrast sharply with the spirit and purpose and procedures and institutions of the Promotion of Access to Information Act, 2000.

The national security debate and its implication for security sector governance

As I have argued in the preceding chapters, the debate about the tension between secrecy and transparency is part of a set of wider concerns about democratic accountability of the security services in democracies. In turn, these concerns relate to how national security is conceptualised and advanced by a society and its government. The debate on national security has been influenced by assumptions and world views of the different proponents. In the Western world, conceptions of national security have been an important dimension of international relations theory in the Cold War period. The Strategic Studies School of analysis, operated essentially within the Realist framework, and was concerned as the name suggests, with the study of strategy (Garnett, 1970). The Realist framework essentially held that states are sovereign and independent entities, acting out of self-interest, and carrying strong potential for conflict with other states (Walt, 1999). Beaufre (1965) described strategy as "the art of applying force so that it makes the most effective contribution towards achieving the ends set by political policy" (1965:22).

The proponents of the Strategic Studies School invariably found themselves taking sides in an essentially bi-polar world, where the main objective of the two leading protagonists in this relationship – the USA and the Soviet Union - was to acquire the lead in the race for nuclear dominance. In countries of the West, a growing number of prestigious academic institutions attempted to carve niches for themselves in the support of governments and their military establishments. Intelligence services of the countries of the East and West found themselves engaged in their countries' attempts to secure influence. These relations were typified by the conflict between the CIA of the United States and the KGB of the Union of Soviet Socialist Republics (USSR). Intelligence services around the world found themselves in the sphere of influence of either of these two well-resourced giants in the world of spying, often serving as satellites of one or the other (Ray, 1979). In the West, the dominant objective was that of deterrence - preventing the extension of the influence of the communist East bloc countries, particularly in the Third World, and ensuring that powerful Western countries remained dominant in the nuclear arms race.

Freedman (1991) observed that the Strategic Studies School underwent a period of crisis, in as far as its capacity to propose viable and lasting solutions to the problems between East and

West, was concerned. The means of war – nuclear arms – being built up by both sides, only served to heighten the political tension between the two superpowers, rather than defuse it. Kaldor (1991) points out that this has to do with the fundamental shift in the nature of military conflict that had taken place in the context of the Cold War: unlike the earlier periods when it was realistic and possible for one state to dominate another through military means, defence strategies and postures were being assumed in this period on the basis of perceptions about the strengths of the opposition.

The Realist approach was countered, particularly from the late sixties and seventies onwards, by a rise in Peace Studies alternatives. Peace Studies analysts called for an end to the arms race, and their arguments resonated with the non-aligned countries of the world, multilateral international organisations such as the United Nations, and a proliferation of social groups such as the women's movement, the green movement and trade union movements. Galtung (1984), a leading proponent of the Peace Studies School, provided an analysis of what would make European nations feel secure. The first variable was the extent to which a country had a credible, non-provocative defence system; the second was a state of non-alignment with any superpower; the third variable, Galtung argued, was a country's ability to be self-reliant in providing for its resource needs; and the last variable, was the extent to which a country's non-aggressive status was considered of benefit to other states.

In the years since the Cold War, the notion of human security has gained currency and persuasion. This promotes a notion of international security as being more than the narrow defence of state interests and territory by primarily military means (Nathan,1992). The term human security gained prominence through its usage in the 1994 Human Development Report of the United Nations Development Programme (UNDP). The report argued the need to re-insert the common concerns of ordinary people who sought "freedom from fear" and "freedom from want" in their daily lives.

The report identified seven elements contributing to human security: economic security (e.g. freedom from poverty); food security (e.g. access to food); health security (e.g. access to health care and protection from diseases); environmental security (including protection from environmental pollution and degradation); personal security (including physical safety from torture, war, crime, and domestic violence); community security (e.g. the physical security

and protection of the identities of cultural and ethnic groups); and political security (namely the enjoyment of political and civil rights, such as freedom of expression). There has been some concern that the expansiveness of the concept of human security makes it ineffective as a theoretical construct, and some sympathy could be had for such an argument, if it is taken into account that intelligence services in post-Cold War period have turned their attention to countering threats to all these elements of security (Todd & Bloch, 2003).

That which makes an issue a security issue may be at the heart of reaching a resolution of the debate on what should be addressed by intelligence services, and subjected to extreme secrecy measures. According to Buzan, Waever & deWilde (1998) something is defined as a security issue when it presents an existential threat to another entity. Invoking security opens the way for the state to mobilize whatever means are necessary to address a threatening development. They argue:

> In theory, any public issue can be located on the spectrum ranging from non-politicized (meaning the state does not deal with it and it is not in any way made an issue of public debate and decision) through politicized (meaning the issue is part of public policy, requiring government decision and resource allocations or, more rarely, some other form of communal governance) to securitized (meaning the issue is presented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure.
>
> Buzan, Waever & de Wilde (1998:23)

The writers argue that these issues may in fact become institutionalised as security issues. An example is intelligence budgets. In practice the issue becomes a security issue not really because a real threat exists, but because releasing information about the budget is presented as such a threat. Implicit in the use of security measures by the state (including secrecy), is the notion that certain categories of information cannot be subject to the normal rules of political conduct, and must be addressed in a realm of extreme politics, namely "securitization" (Buzan, Waever & deWilde, 1998). A further assumption is that society's access must be

controlled, regulated and even subject to punitive measures, because such access might undermine the very structures and regulatory capacity of the state. By "securitizing" certain issues, the state assumes it represents the interests of all who are its subjects, and uniformly applies its requirements, including the upholding of its secrets, to all. Securitizing an issue, however, does not mean that this act is accepted by all, and in the literature, securitization is used to refer to that condition where there is general acceptance that an issue should be dealt with outside the ordinary rules of political conduct.

Buzan, Weaver & de Wilde, 1998) are critical of the silencing effect of "securitization", and argue that it can have a harmful effect. They warn:

> ….National security should not be idealised. It works to silence opposition and has given power holders many opportunities to exploit 'threats' for domestic purposes, to claim a right to handle something with less democratic control and constraint….Basically, security should be seen as negative, as a failure to deal with issues as normal politics.
>
> Buzan, Waever & de Wilde (1998:29).

In concluding this section, we need to take note of how, following the attacks on the World Trade Centre and other US installations on 11 September 2001, new approaches to national security have impacted on the rest of the World. With immediate effect, the administration of President George Bush, in its role of sole superpower began mobilising global support for what it dubbed the "war on terror" (Lansford, 2002; Schneier, 2003; McGoldrick, 2004). In its own environs changes included the allocation of billions of dollars towards improving its defensive capacity; and a review of the security and intelligence capacity that in the establishment of an Office for Homeland Security.

Freedom of information advocates were alarmed by the tightening of controls over information and restrictions imposed on society so antithetical to the "American way of life". The conditions of heightened alarm breathed new life into security and intelligence services in the Western world, where budget were injected with additional resources to combat the

terror threat. By the time the USA launched its war on Iraq two year later, for its alleged development of a chemical and biological warfare capacity, which the USA and its major ally, Britain, claimed would be used by Iraq to further the cause of international terror, the world had been polarised, into supporters and opponents of the war. In contrast to the adherents to the school of thought that held that terror had to be combated by military means, there were those governments that held that the only lasting solution in such a scenario was a political one, and that the role of multilateral institutions should be strengthened to play this role. Subsequent events – the war which claimed many lives but did not reveal the existence of a nuclear warfare capacity, the institution of a transitional authority in Iraq by the USA, the escalation of a low intensity conflict between coalition forces and armed combatants - have disproved the theory that military means would achieve stability. For many, the war was seen as a convenient but transparent excuse to effect an imposed regime change (Scraton, 2002). That the war appears to have been embarked upon on the basis of intelligence lacking in credibility, strengthens this perception. Both in the USA and the UK, public debate has raged about the role of the intelligence services, most descriptively put by the allegation that policy-makers took the decision to go to war based on analytically weak intelligence reports. Overall, the world does seem a more uncertain place calling for more sophisticated analyses and responses to its many conflicts.

National security in Africa and the Third World

The era of the Cold War was characterised by intensive spying and governmental secrecy. Around the world, newly formed intelligence services consolidated themselves around the main protagonists in the ideological battle, the USA and the Soviet Union. Africa did not escape these alignments. Modern African states had their origins in the colonial partition which took place at the Berlin Conference of 1884 (Smith, 1983). In the carving up of the continent that characterised this "Scramble for Africa", the needs and aspirations of Africans were largely ignored, and the administrative structures created by the Europeans were mainly designed to facilitate their access to the natural resources of the continent. National identities were imposed on Africans, with historically specific identities and the heterogeneity of African societies being ignored or misunderstood by the colonialists. Very often the only factor uniting the colonial entities was that the African people in a common territory were subordinate to a single colonial power. Ironically, because of the common experience of

colonial oppression, a sense of nationhood developed among the people thus brought together, resulting in resistance movements, and a clamour for independence from colonial rulers (Smith, 1983).

When independence came, however, many of the administrative structures remained intact, or were modelled on the colonial variants, even where Africans filled the positions. Post-colonial intelligence services were often merely a reflection of the core-periphery relations, even after nominal independence from colonial powers had been attained. Africa was therefore drawn into the Cold War conflict between West and East, the chosen attachment a reflection of a state's ideological alignment, and the availability of support from the East or West.

Third World writers have tried to locate themselves as operating from a different set of assumptions from those of Western countries when discussing national security. Azar & Moon (1988) argue that:

> National security is a Western, largely American, concept that emerged in the post-World War II period. As the burdens of the presidency of the United States grew heavier and American involvement in international affairs grew deeper, the structure and management of policy-making at the national level required new and bold approaches. As the international environment grew in complexity, and it became necessary to integrate military, diplomatic, intelligence, technological, economic and other diverse data at the apex of American decision-making, the American President in 1949 launched the national security apparatus.
>
> Azar & Moon (1988:1)

This apparatus included the intelligence and defence community of the USA, including its industrial military complex. Not only was it matched by a similar reaction from the USSR, the militarised footing of these two giants affected the rest of the world whose national

resources also tended to be directed to security imperatives. According to McLaurin (1988) and Azar & Moon (1988), one invalid assumption often made about the developing world, particularly during the Cold War era, was that the nation-state was a homogeneous entity, in which the security of the people could be equated with the security of the state. Another invalid assumption was that the citizens within a common geographical area automatically shared a common destiny and interests, because of the extended process of nation-building and a common political socialisation. Numerous examples attest to the fact that these assumptions, whilst largely true for the western world, simply did not hold true for the less developed countries. In many unstable countries, national security was equated by the ruling regime with their own tenure, and they in turn represented a segment of social and political interests.

Analytically, it is useful to situate an assessment of governance over the intelligence services in Africa, in the context of the debate on security sector reform, a construct which has emerged since the 1990s as a powerful organizing force among international and African actors dedicated to conflict prevention and poverty reduction, notwithstanding differences in outlook on the problems and their solutions (Rupiya, 2004). There is broad consensus that the factors that define meaningful security sector reform include democratic or civilian control of the security services, legislative oversight over their activities, transparency and accountability in the management of the security sector, and regional security arrangements that emphasis cooperation rather than competition between neighbouring countries (Born, 2003; Le Roux, Rupiya & Ngoma, 2004).

Lala (2004) acknowledges that certain programmes that are undertaken in the name of security sector reform in Africa have been donor-driven, making it difficult, sometimes, for African states to determine their own agendas. Notwithstanding this factor, security sector reform has had positive spin-offs that can consolidate the democratization processes through which so many African countries are going. There is a formal requirement that compliance with the rule of law, oversight and accountability mechanisms will replace former scenarios, especially where the security services may have played a significantly politicized and partisan role. Typically though, there are problems derived from the legacies from which the political systems have emerged:

> The extent to which oversight is exerted is limited by the fact that members of parliament (MPs) are subject to strong party control and thus allegiance to the party rates higher than ensuring the rights and needs of their constituents. A number of African parliaments also suffer from a low profile in terms of their legislative function. In the area of security, where specific expertise in necessary, the respective Committees often simply accede to the proposals by the Executive.
>
> Lala (2004: 10)

Oversight of the intelligence services in African countries is especially challenging and controversial, since there is a strong tradition of autonomy on the part of these structures. Lala (2004) contends however, that mechanisms can be put in place to ensure that parliaments have access to information about their activities. The debate on effective governance of the security forces, especially the intelligence services, is not confined to South Africa.

Aguero (2004) too, describes the security agencies and military and police institutions inherited from authoritarian regimes, as being adept at survival and "re-accommodation" within new democracies that have resulted from negotiated transitions:

> Security forces retained high levels of autonomy and prerogatives, as well as practices that contradicted democratic norms. Developing institutions that rein in these tendencies and assert control is one of the primary tasks of these new democracies. In cases where democratization followed the settlement of armed conflict, officials have had to wrestle with the more complex challenge of recreating institutions whilst simultaneously providing for citizen security.
>
> Aguero (2004:3)

Aguero (2004) points out that the problems facing the armed forces, the police and intelligence agencies are mutually reinforcing. A weak or ineffective police service will put pressure on officials to use the military in policing roles for which it is poorly prepared, or to militarise the police. Certainly, the issues raised by Aguero (2004) are relevant to this study,

since they are similar to the questions that faced policy makers with the establishment of the post-apartheid security dispensation. He asks what the most appropriate institutional settings for asserting effective and democratic control over the armed forces and the security services are. Further, how should different kinds of security threats is confronted in ways that lessen opportunities for state security services (or at times even key elected officials) to engage in actions that undermine democratic institutions and practices? Aguero (2004) also urges analysts to explore the various modes of civil society participation that may help strengthen democratic institutions in the security sector.

The establishment of the African Union (AU) has brought African countries together to forge their own collective path a in the face of global economic challenges, commonly experienced by African states. Institutions of multilateral governance include an African Parliament and a projected common currency, both reminiscent of the path being undertaken by Europe. Yet to deny that there are contradictions within this broad stratum would be naïve: the interests at play even within regional formations such as the Southern African Development Community (SADC) and the Economic Community of West African States (ECOWAS), are sometimes quite disparate that finding a common platform on the question of security can only be a huge challenge (Cilliers, 2005).

National security, security sector reform and access to information in South Africa

Various empirical and analytical studies of the conceptions of national security under apartheid were undertaken in the eighties and nineties when apartheid was finally dismantled (Cawthra, 1986; Grundy, 1986; Cock & Nathan, 1989; Nathan, 1992; Seegers, 1996). Much of the debate has been influenced by liberal thinking on the morally reprehensible nature of apartheid; in addition, the peace studies approach and critical theory – a body of theory which questions the state-centred approach of the realist paradigm - have also been influential. The apartheid security doctrine is probably most cogently captured in security legislation passed through the years. This legislation was the basis of thousands of repressive acts, many of which have only come to the public attention since the investigations conducted by and representations made to the Truth and Reconciliation Commission (TRC). Well known to the public however, were the restrictions on anti-apartheid organisations, detention without trial,

political trials and imprisonment, and suppression of protest action and the media (Mathews, 1971, 1978).

National security was seen by the apartheid government in terms of the South African state's ability to counter the Soviet "threat" and this was writ large in its policies. Beaufre and McCuen (the latter espousing an "art of counter-revolutionary warfare") featured prominently in the training doctrine of the South African Defence Force, and their strategic approaches pursued in governmental policy (Cawthra, 1986). The 1977 White Paper on Defence called for a multifaceted defence strategy, co-ordinated on a number of fronts including the economic, social, psychological, ideological, technological and cultural. This implied the involvement of a wide range of departments and resources mobilised in defence of the state, which should not be seen as the responsibility solely of the defence force. The discourse of national security as expressed under apartheid was challenged by critics of the apartheid government. The eighties contributions to the analysis of the security establishment centred on the National Security Management System, a multi-pronged strategy aimed at securing the country against internal and external threats (Swilling & Phillips, 1989; Hansson, 1990).

Academics and analysts sympathetic to the non-racial democratic movement in the early 1990's interacted to share and develop mutual perspectives on different aspects of transforming institutions in the security sector, that could feed into the process of negotiating a political settlement (Chuter, 2000). In the debate around the future of the security forces and a redefinition of their role, two such groups were the Military Research Group and the Policing Policy Group. Other institutions contributing to this debate included the Centre for Defence Politics and the Centre for the Study of Violence and Reconciliation. Very often this academic role was coupled with an activism in the transformation process, also a defining feature of security studies in South Africa. Not surprisingly then, many academics of this generation have gone into positions in government, where their attempts to translate their policy ideals into effective measures to transform the security force, are now being played out.

Following the long years of oppression by the security forces under apartheid, security sector reform - or transformation - has had its own dynamic, but was influenced by the debates in other parts of the world and continent, about the need for democratic control of the security

services. The outcome of the political was such as to guarantee the integration of the notion of human security into the post-apartheid Constitution. This laid the basis for an overhaul and alignment of the security sector structures with democratic principles, and legislation to give effect to the principles of oversight and civilian control over the security services (Cawthra, 2003).

In recent years across the world, the challenges for intelligence services have been compounded, and the temptation to restrict access to information is made greater by the perception that information about the state made too freely available could be used to terrorise a country and its citizens. In the post 9/11 period, some of the focus has shifted to how security governance may have to be reconciled with an uncertain world, the perception of a terror threat looming large in this analysis (Lansford, 2002). This world view does not go unchallenged, and some analysts academics have contested the undermining of global institutions of governance, whilst others have gone further and argued that the motives for creating the perception of a threat, have much to do with the economic designs, cultural biases and global political agendas of those pressing for military conflict (Hauerwas & Lentricchia, 2003).

For South Africa, whose democratic institutions are relatively new, the durability of the above-mentioned security sector reform is a grave consideration, in ensuring that the security services do not revert to conditions of unaccountable behaviour. A key lever in this debate, will be the degree of public participation and interest, to guarantee that the gains of the new dispensation are secured. State institutions by their nature, are powerful entities, and if their access to resources, information and power is not offset by public vigilance, the consequences could be disastrous (Mathews, 1978). Closing in on free access to information, in this context, can be seen as a form of securitization, as conceptualized by Buzan, Waever & de Wilde (1998), who argue that security in general, is indicative of society's failure to regulate itself in an equitable way. Securitization of political issues, in other words, subjecting them to the sphere of control of the security services, illustrates that the normal processes of politics have failed. The role of oversight bodies in countering the power that security services have, is therefore critical (Modise, 2004).

Concluding remarks

What emerges from a review of the literature is that managing the tensions between secrecy and transparency in a democracy is often a complex task (Bok, 1982). The entrenchment of a constitutional right of access to information has been a defining feature of the post-apartheid political landscape, and is in keeping with international trends in democratic political systems. However, in international law, the duty of states to protect their secrets has also been a long-recognised principle (Evatt, 1999; Nichols, 1999). Whilst this is also the case in the South African context where access to information legislation co-exists with legislation protecting other information, the academic literature in South Africa has tended to focus on the constitutional right to know, rather than the right of the state to protect information from disclosure where national security considerations justify this (Mathews, 1978; Currie & Klaaren, 2002). This polarisation of the policy debate suggests that there is no consensus between the intelligence services and important stakeholders in the public domain on what constitutes a threat to security and what information therefore warrants protection. Currie & Klaaren (2002) for example, argue that it is problematic that the Protection of Information Act, 1982, is retained on the statute books, when the Promotion of Access to Information Act, 2000 provides a right of access to information, and grounds for refusal of access to information.

Most liberal writers on the subject are in agreement that transparency can be leveraged to give citizens access to information important for them to defend their rights, and to give marginalised groups meaningful insight to the workings of state (Mathews, 1978). This is so with the security institutions, given the sensitivities of managing secrecy in a democracy (Adler, 1991; Lustgarten & Leigh, 1994). However, as Robertson (1999) points out, access to information legislation around the world has not resulted in significant shifts in power relations, and must cause us to consider whether it is a panacea for poor government. It appears not to be, and therefore any remedies for governance of the security sector should include a range of oversight and accountability mechanisms.

Many would argue that because South Africa is not in a state of heightened and adversarial conflict, it does not require the resort to extreme secrecy, such as that which characterised the apartheid period or the Cold War. However, it is increasingly accepted that the world, apart from being interconnected, is fairly unpredictable and there is still a variety of threats for which the early warning capabilities of intelligence services are required. Most useful have been the analyses of transitions from authoritarianism and the role of the security services therein (Cawthra & Luckham, 2003). This demonstrates that each transition is unique: South Africa's arose out of a politically inclusive process; moreover, the fundamental principles concerning the role of the security services have been incorporated into the country's Constitution.

The danger in treating matters of political differences, as security matters is best encapsulated in the concept of "securitization"(Buzan, Waever & de Wilde, 1998). They warn that a heightened sense of security can lead to security resources being deployed in addressing conflicts which in fact require normal political interventions. Again, this related to the perception of threats, which is the basis on which intelligence services are employed. A focus on human security is clearly more suited to addressing the challenges of the twenty-first century, calling as it does for co-operation rather than subversion and spying.

The literature review shows that there has been important work around the significance of access to the records of fallen authoritarian regimes, when this becomes possible under a change of government. Such access is of enormous social and political value, and allows a society to come to terms with its past, particularly the past role of its security forces. This is pertinent to South Africa, where the Truth and Reconciliation Commission revealed a systematic destruction of state records (Posel & Simpson, 2002). Because the archival record is not a neutral entity, it should be viewed as only one representation of reality, which is also continuously shaped by non-state actors through other forms of recording memory. Particularly relevant is the case of intelligence records which continue, after apartheid to be subject to much control and secrecy. Opacity around state information holdings which are not readily accessible to the public raises the spectre about the vulnerability of these documents to distortion and even disposal, all possibilities when governance mechanisms are not effective. In practical terms, and for transparency to be given meaningful effect, the full

weight of countervailing systems, including oversight of intelligence should be brought to bear.

CHAPTER FOUR

OFFICIAL SECRECY AND STATE SECURITY UNDER MINORITY RULE IN SOUTH AFRICA

Introduction

This chapter presents an overview of the system of official secrecy and state security under white minority rule. The review begins at the turn of the twentieth century, and covers the period till February 1990, when the African National Congress (ANC), the South African Communist Party (SACP), the Pan Africanist Congress (PAC) and other banned organisations were declared lawful organisations again. The policy context for secrecy in the years under review was the objective of successive white governments of leveraging their political and economic dominance to exclude blacks from participating in the economic and political mainstream, and to entrench a racial notion of South African citizenship. The system of state secrecy went hand in hand with an agenda of repression. In this chapter, I analyse the relationship between these secrecy measures and the systems of political control and domination. My intention is to illustrate that security and intelligence services have an enormous propensity to abuse their power, if they are not subject to public scrutiny.

A number of significant phases during which official secrecy was crafted and implemented can be discerned. Whilst I have divided the period into five phases, that seem to define shifts in the state's approach to security, other periodisations are possible. My brief description of the period prior to Union in 1910 is intended to show that a sense of being under threat prompted both Boer and Briton to establish institutions that would provide early warning on matters that threatened their interests. The period 1910 – 1945 covers the year that South Africa's four white-controlled colonies merged to become one Union under a central government that owed its allegiance to the British crown, up until the end of the Second World War. 1945 – 1960 covers the period in which the Afrikaner-based National Party was voted into power, and began a process of consolidating racially exclusive and segregationist policies. The section on the years 1960 – 1976 cover the banning of the liberation movements by the government and their subsequent resort to an armed struggle, till the year in which

students led the national uprisings that began in Soweto. Finally, 1976 – 1990, a period of mass political resistance, was characterised by heightened repression on the part of the apartheid government; this included a "State of Emergency period", and the deepening political crisis of the apartheid government, in which it became apparent to them that exploring a negotiated political settlement with the liberation movements was necessary to bring political stability to South Africa (Gerhardt, 1978; Davidson, et al.; Magubane, 2004).

A detailed study of the history of secrecy and state security should examine for each period, the policy imperatives of the government of the time, the legislative context for secrecy, the administration of the system of secrecy, the shape of the intelligence and security forces, and the manner of resistance that ensued against secrecy and repression. It is meant to provide a background to understanding the post-apartheid South African secrecy system, and sketches very broadly the origins of contemporary policy, and its flawed political basis, which resulted in its legislative and administrative shortcomings. Although mention is made of the secrecy system from 1910 onwards, the emphasis is on the apartheid era, since it was the legacy of successive apartheid governments that had to be undone when democracy was formally attained in 1994. A more comprehensive account would have done two things: the first is to locate the development of the secrecy system in South Africa in relation to the development of the peculiar nature of capitalist domination, and recognise the role of race and class in this equation. The second would have been to analyse in detail the struggles of the people of South Africa in shaping their destinies and resisting the forms of control which various minority governments sought to impose on them. It is to be hoped that the study is not significantly poorer for omitting details of these areas of research, and that the overview of secrecy is sufficient to locate the contents of the subsequent chapters, which deal with the transition to democracy and the impact of a more transparent political system.

The period prior to 1910

The official structures of white rule in the territories that were later to constitute the Union of South Africa faced, in their opinions, hostilities sufficient for them to employ secret agents. Blackburn & Caddell remark that secret service in South Africa pre-dated the Union of 1910:

> In the early days of political stress in the Cape Colony, a system of secret intelligence was developed automatically, particularly at the period of the British occupation, when the Boers were becoming restless, and the growing discontent manifested itself in more or less open meetings at remote farms, and secret mutterings in the market place, or at the great quarterly religious gathering, Nachtmaal.…It is justifiable to say that the men and women of the South African Colonies who have acted as secret conveyers of information to governments or their representatives have, in the vast majority of cases, been actuated by something sufficiently far removed from sordid motives to warrant its being accounted to them for righteousness, if not for the purest patriotism. This is probably true of the men – and women – who assisted both sides during the last Boer War.
>
> Blackburn & Cadell (1911:3)

The issues around which secrecy and espionage manifested, the authors elaborated, went to the heart of control over resources and subjugation of the indigenous people: the illicit liquor trade, gun running, and the smuggling of precious minerals (Blackburn & Cadell, 1911). On the formation of a Boer secret service, these authors described the role of Dr William Leyds, who became Secretary of State of the Transvaal Republic after serving an initial period as a prosecutor. Leyds, a brilliant young Netherlands man who just completed his legal studies, was recruited by a scout who recommended him to President Paul Kruger. There was considerable sympathy in the Netherlands for the Boers during their wars against the British, a sentiment shared strongly by Leyds who had little hesitation in taking up the offer put to him by President Kruger to take up a post as a prosecutor (Van Niekerk, 1985).

Van Niekerk underlined just how strategic a role Leyds occupied when he became Secretary of State:

> *Die kantoor van die staatsekretaris was dus die skakel tussen die Volksraad, die regering en alle staatsdepartemente. Naas die president was die staatsekretaris die vernaamste administratiewe amptenaar wat verantwoordelik was vir die uitvoering van alle besluite van die Volksraad en Uitvoerende Raad. Namens die staatspresident moes die staatsekretaris alle lede van die twee rade skriftelik in kennis stel van*

> *sittings en lede wat sonder grondige redes afwesig was, oorenkomstig grondwetlike bepalings beboet. In die afwesigheid van die staatspresident moet die staatseketaris hom in die Volksraad verteenwoording. Die staatsekretaris was ook belas met die sakelys van die uitvoerende raad en het in die raad opgetree as sekretaris totdat 'n afsonderlike notulehouer in ongeveer 1892 aangestel is.*
>
> Van Niekerk (1985:64)

Under Leyds's guidance, an organised system of secret service also developed:

> When the Kruger Executive began to realise that European opinion was a thing that mattered, and that the South African Republic really had a foreign policy and foreign relations like other respectable and old-established countries, then, and not till then, was a separate account voted and kept for 'informatie'. Within ten years the secret service of the Transvaal developed from a primitive affair of private inquiries….. to one of the most expensive and extensive in the world.
>
> Blackburn and Cadell (1911:237)

A charismatic figure, Leyds placed great store in communications in his central role, and developed an extensive network of contacts in the media in Europe. He sought to influence opinion in favour of the Transvaal Republic. The outlook was probably not unlike that which obtained in the British Empire, which in addition to being the wealthiest and most powerful nation in the late nineteenth century had a network that ensured that the Crown was well informed of all developments in the realm.

Modern South Africa's history of official secrecy can be traced back to the formation of the Union of South Africa in 1910 through the South Africa Act, 1909, which was passed by the British parliament (Bindman, 1988). The unification of the two former Boer Republics (Transvaal and the Orange Free State) with the British-controlled Cape and Natal colonies was preceded by a National Convention which sought to find agreement on how whites could co-exist in South Africa, while excluding blacks from the political mainstream. The exclusion of blacks from the Union's political and economic mainstream was to be the core element of

domestic security policy of successive white governments. At the heart of the strategy of those in power was to ensure that the demands of white workers were carefully managed, while ensuring that the benefits of economic inclusion did not extend to the Union's black majority. Often, the authorities made use of organised force to uphold this strategy.

1910 - 1948

During the period 1910-1948, the Union of South Africa was subject to British legislation prescribing official secrecy. An Official Secrets Act had first been passed in Britain in 1889, and was repealed and replaced in 1911 by an amended Act. According to Mathews (1978), the Act may have been a response to leaks of official documents relating to foreign affairs, including a leak about a secret treaty between the United Kingdom and Russia in 1878. The law prohibited British citizens from disclosing state secrets, thus the basic crime was communication of official information, and not espionage. This limitation was addressed with the introduction of the replacement Act, which appeared to have espionage in mind, but which nevertheless had as its focus the penalising of those who disclosed official information.

The Official Secrets Act was thus passed in South Africa in 1911, and other British dominions, including Australia, New Zealand and India in the early twentieth century (Mathews, 1978; Geldenhuys, 1984). Subsequent amendments passed in Britain, however, were not incorporated into the South African legislation, with the result that the law remained unchanged until it was repealed and replaced in 1956. The British Official Secrets Act, covered the crime of spying, committed by anyone who endangered the safety or interests of the state by engaging in any one of three activities: approaching, inspecting, passing over, entering or being in the neighbourhood of a prohibited place; or making a sketch, plan, model or note which might be or was intended to be useful to an enemy; obtaining, collecting, recording, publishing or communicating to any other person, documentary or other information which might be directly or indirectly useful to an enemy.

In addition, the Act made it criminal to use official information for the benefit of any foreign power or in any other manner prejudicial to the safety or interests of the state. It was also a crime for a person with possession or control of information that related to munitions of war to communicate it directly or indirectly to any foreign power or in any other manner

prejudicial to the safety or interests of the state. It was also a crime for a person to retain for any purpose prejudicial to the safety or interests of the state any official document when the accused has no right to retain it. (Mathews, 1978).

With the formation of the Union, more significant than the relations between white South Africans and Britain, was that blacks were excluded from political life. Government was not accountable to this majority, which included a peasantry that was being forced off the land, a growing unskilled class of workers, and politicised but small black elite (Gerhardt, 1978). Each of these groups responded to their marginalisation through varying forms of protest. Collectively, the resistance of the peasants, who revolted against their dispossession of their land, the workers who clashed with white miners in the urban areas, and the black elite who petitioned the overseas centres of power in protest against their political exclusion, shaped the early Union government's domestic policy. This policy in essence was resolved in favour of white workers by their incorporation through labour policies that gave them preferential treatment. This overall approach was the response of government to the major security issue of the time, often referred to as the "Native question" (De Kiewiet, 1941).

Matters of foreign policy were rarely debated by Parliament in the early days of the Union and decisions were often taken at Executive level. Notwithstanding this, international relations constituted an important part of the Union government's survival strategy. The Information Service, which fell under the Department of External Affairs, was the channel of foreign representation. Initially, South Africa had no independent international status, and foreign relations of the dominions were handled directly by the British government (Geldenhuys, 1984). The 1926 Balfour Declaration defined the relationship between Britain and the dominions as being between autonomous communities within the British Empire, equal in status, except in the spheres of foreign affairs and defence, which would remain the responsibility of the British government (Geldenhuys, 1984).

The consolidation of white political power was characterised by the establishment of security institutions that unified the former components of the various colonies and Boer Republics. The Union Defence Force (UDF) and the South African Police (SAP) were faced with the task of integrating disparate security cultures and welding them into one. Seegers (1996)

notes that through these institutions, the system of secrecy developed early. Both the Botha and Smuts governments focused the attention of the SAP on Bolshevik elements in the trade unions. Between 1910 and 1920 the British police's work was also drawn to the activities of the British Communist Party and leftists in the labour movement. London and Pretoria shared information supplied by informers. Seegers also noted an early reliance on "black detectives, informers, and trackers in stock theft cases, who were praised for their zeal" (Seegers, 1996:51).

The period after the First World War up till the Second World War saw the development of informal institutions aimed at consolidating the position of the Afrikaner in society. The formation of the Broederbond in 1918, as an institution aimed at consolidating Afrikaner aspirations, was one such initiative. In the 1940s, pro-Nazi supporters formed the Ossewa Brandwag (OB). Some of its members were later to be recruited into the first formal, civilian intelligence organisation, the Bureau for State Security, when it was constituted during the term of Prime Minister B.J. Vorster, in a later period (Grundy, 1986). Seegers (1996) observes that the SAP was the first security agency to respond to the information-gathering needs of the war, when it was ordered to intervene in the face of a significant show of pro-Nazism in the then territory of South West Africa.

The infringement of personal liberties was an integral part of the Union's machinery of secrecy and state security. Mathews (1971) notes that in the First World War, detention and imprisonment were provided for in the Indemnity and Special Tribunal Act of 1915, and that similar measures could be effected in terms of the War Measures Act during World War Two. In both cases, these war measures were withdrawn after the cessation of hostilities; however a similar measure was applied to blacks almost as a matter of course:

> A section of the Natal Bantu Code which empowers the detention of African (Bantu) persons without trial has been a long-standing exception to the temporary nature of such provisions. The provision authorizes the Supreme Chief (State President) to order the detention of any African if he is satisfied that he is a danger to the public peace.
>
> Mathews (1971: 131).

Mathews (1978) cites examples of the application of the Official Secrets Act during the Second World War. In R. vs Wentzel, the accused was acquitted on charges of having written, and placed in an envelope ready for posting to an address outside the country, information which might have assisted a foreign power. South Africa at the time was at war with the Nazi alliance. The defence of the accused was that he had not intended to post the information, but had held it in reserve, should he have had to explain himself to a victorious Nazi government, which seemed to him a probability at the time. Significantly, the accused was acquitted because the state had failed to prove his intention to communicate the contents of the letter. In another case, R. vs Vorster, the state was successful. The accused, it was found, had collected information about the number and calibre of guns at the naval base in Simonstown and the reliability of the personnel stationed there. The court, in this case, accepted that because the information had been obtained from a person not authorised to communicate it, it "brought into play the presumption that an accused who had so obtained information was acting for a purpose prejudicial to the safety or interests of the state" (Mathews, 1978:140).

In summary, it can be said that considerable official secrecy measures then, were in place in the period 1910-1948, the main legislative vehicle being the Official Secrets Act of 1911. Domestic and international imperatives drove the state's priorities when it made use of secrecy legislation: these included the imperatives of the new Union: addressing the "Native question", controlling the growth of the working class movement, and assisting the Allies in the Anti-Nazi war efforts. The institutions that developed out of this effort had some of the hallmarks of modern security organisations, but were overshadowed by the factor of racial exclusivity, which became more pronounced after the ascent to power of the National Party (Grundy, 1986; Cawthra, 1986). The British influence was particularly strong in shaping security and intelligence policy, and addressing the various threats to Union interests at the time. One perceived threat that loomed large was black resistance, at once a force that shaped domestic security policy, and a factor in shaping the role and orientation of the security forces.

1945 - 1960

In the aftermath of World War Two the international arena was marked by a heightened ideological stand-off between East and West, in the form of the Cold War. In line with global trends, intelligence services became a more dominant feature of the South African political landscape after World War Two. The Security Branch of the South African Police was established in 1947. Drawn from the detective service of the South African Police, the Branch acted as an elite political police. In its internal security function, it was engaged primarily in tactical intelligence activity. Intelligence was gathered mainly about political opponents of apartheid, and aimed at achieving short- and medium-term objectives such as detentions, prosecutions and imprisonment.

South Africa's foreign relations in this period were a response to the country's increasingly isolated position, and had to be conducted in an increasingly stealthy manner. Gone was the international stature and prominence that Smuts had achieved during his tenure as Prime Minister, a position that saw him serve as a member of the British War Council. The role of information officers posted abroad by the State Information Office was to "combat the hostile propaganda of South Africa abroad" (Geldenhuys, 1984). The number of information offices abroad multiplied – by 1953 there were fourteen, and several restructurings of the bureaucracy in South Africa resulted in the establishment of the South African Information Service in 1957. The role of the Information Service was to influence foreign opinion in favour of South Africa's domestic and foreign policies. In this period, the United States, Britain and Western Europe were singled out by South Africa as priority areas for winning support for its policies. Africa was not a high priority with only one office in the "north", in Salisbury in Southern Rhodesia (Geldenhuys, 1984).

In 1948, the National Party was voted into power by the white electorate. Its ascent to power was marked by policies and legislative measures to enforce racial separation and white privilege in all walks of life (Grundy, 1986; Bindman, 1988; Van Diepen, 1988). The system of apartheid needed strong measures to ensure compliance in a black population that was increasingly defiant, and the period after 1948 saw the establishment of the security services and a rash of legislative measures designed to enforce the Nationalists' apartheid doctrine

(Bindman, 1988). Apart from legislation explicitly aimed at countering resistance – or "communism" as the framers often insisted on calling many forms of protest– there was a trend of other many areas of public life being subject to sweeping secrecy from the time the National Party gained power. The Wage Act of 1957 for example, prohibited wage board members and other officials from disclosing to the public information acquired in the course of their duties, thereby placing severe limitations on trade unions' ability to function. Wide restrictions on disclosure were also contained in the Industrial Conciliation Act of 1956, the Bantu Labour Relations Act of 1953, and the Reserve Bank Act of 1944 (Mathews, 1971).

The laws introduced by the National Party government included many intended to suppress freedom of expression and political association. They included the Suppression of Communism Act, 1950; the Internal Security Act, 1950; the Public Safety Act, 1953; the Riotous Assemblies Act, 1956; the Defence Act, 1957; and the Police Act, 1958. The domestic political context in which these legislative changes took place was one of increased black opposition to white rule (Gerhardt, 1978; Davidson, et al., 1976). This opposition was largely peaceful, though mass-based, and was characterised by increasing union between different racial groups. In the Cold War context, resistance to white rule was labelled as Communist, and the barrage of legislation passed in the early 1950s was predicated on this assumption.

Mathews (1971, 1978) compares and contrasts with South Africa's experience, the introduction of legislation in countries which placed restrictions on political association and access to information in the early part of the twentieth century. Like the United Kingdom, the United States had first introduced its Espionage Statutes in 1917, the main thrust of which was to define the crime of espionage as the communication of documentary or other information relating to national defence, to a foreign nation or agent, knowing or believing it could be used to the detriment to the United States, or to the advantage of a foreign nation. The United States was also one of the few Western democracies that had an extensive anti-communist legislative programme, which entailed the suppression of the basic freedoms of expression, of information, and intruded on the privacy and liberties of those subject to the legislation (Mathews, 1971).

In the United States, the Smith Act of 1940 was introduced to counter pre-war Nazi and Fascist groups operating in the United States. It was used, however, extensively against communists. Other legislation included the Subversive Activities Control Act and its super-ordinate legislation, the Internal Security Act of 1950, and the Communist Control Act of 1954. Mathews (1971) notes that the United States legislation, unlike its South African variants, did not enjoy free passage and that it had to be refashioned considerably to align with the rule of law and requirements of due process. In South Africa, though, semi-authoritarian conditions allowed the passage of laws that routinely restricted information and undermined personal liberties.

South African legislation continued to be weighted towards the suppression of information, rather than allowing public access. Even institutions within "white" South Africa – the media, the Senate and Parliament, and other institutions - were subject to the restrictions that resulted from the security legislation. The Defence Act of 1957 prohibited the publication of three classes of information without ministerial authority, and had the effect of depriving the general public of the right to virtually all information, whether directly or indirectly connected with defence, and further making it a crime for any government employee or contractor, or any person to whom the information had been given in confidence, to disclose it without authority. The three classes of information were:

- information relating to the composition, movements or disposition of the South African or foreign armed force, or their armaments commissioned in terms of the Act;
- statements, comments or rumours about a member or activity of the South African or foreign armed forces, calculated to prejudice or embarrass the government in its foreign relations or to alarm or depress members of the public; and
- secret or confidential information relating to the defence of the Republic, including information about the actual or proposed fortification of defence.

The implications of this last category were wide ranging: in terms of the Act, all information relating to the defence of the Republic was presumed secret or confidential unless the contrary was proved, and any information relating to military equipment was deemed secret unless publication had been authorised (Mathews, 1971).

The Internal Security Act of 1950 served to restrict access to information. It authorised the State President to ban a publication on the grounds that he believed it to convey information calculated to achieve the objectives of communism, or to endanger the security of the state or the maintenance of public order. The review procedure established in terms of the Act was itself subject to restrictions at various levels: its composition, findings and recommendations were never made public, being disclosed only to persons who had a duty to deal with the subject at hand (Mathews, 1971).

Lastly, mention can be made of the Prisons Act of 1959, which also contained provisions that restricted access to information. In terms of the Act, it was a criminal offence to make a sketch or take a photograph of a prison or any portion of a prison or to publish these without the authority of the Commissioner of Prisons. Similarly, photographs of prisoners or detainees could not be taken with the intention of publishing them unless for use in connection with official purposes. Effectively, this Act placed restrictions on making known the poor conditions under which prisoners might be kept (Mathews, 1971). Significantly, these provisions in the law came about after the "Treason Trial" of 1956, in which a large group of anti-apartheid leaders were tried. Their pictures – and their cause – received widespread publicity, which no doubt spurred this newest form of censorship.

1960 - 1976

Increased resistance to apartheid led to further repression and in 1961, the banning of the ANC resulted in the organisation's remaining leadership retreating into exile to consolidate the organisation (Davidson, et al., 1976). The radicalisation of liberation politics also saw the government resorting to more complex measures in their efforts to coordinate intelligence. In 1963, the State Security Committee was created, along with a Working Committee (National Intelligence Service, 1994). Because these structures did not function on a full-time basis, they were largely ineffective. The Working Committee was replaced by an intelligence-coordinating committee, which also had limited impact because the State Security Committee did not meet regularly. In 1966, intelligence coordination again came under scrutiny and the then Prime Minister, H.F. Verwoed, decided that the State Security Committee should be changed to the State Security Advisory Council (SSAC). The latter had a secretariat consisting of members of the intelligence community and was known as the Intelligence

Coordination Division (ICD). With the exception of the Director, the ICD was composed of non-permanent members who were dependent on departmental members for basic intelligence (National Intelligence Service, 1994).

1969 saw the formation of the Bureau for State Security (BOSS). The first head of the Bureau, H.J. Van den Bergh was approached by the then Prime Minister. B.J. Vorster, to establish an intelligence organisation. Cabinet saw the need to be informed about security matters. Initially the proposal of Cabinet was that Van den Bergh would also control the Security Police and Defence Force Intelligence. Van den Bergh explained that he advised the Prime Minister that he could not carry out his order and recommended to him that he appoint Appeal Court Judge H.J. Potgieter of Bloemfontein to investigate the matter. The idea of a new, central intelligence organization had not been met with much enthusiasm by the departmental intelligence services, which feared that it would encroach on their mandates (National Intelligence Service, 1994).

In September 1969, Judge H.J. Potgieter was appointed to conduct an inquiry into the activities of the intelligence departments. The judge's final report was completed in August 1970, and advocated the creation of a Bureau for State Security to investigate and evaluate all matters, whether within the country or abroad, that threatened or had a bearing on the security or safety of the country, and to advise the Prime Minister about these developments. The Prime Minister agreed to the formation of a department, which was known upon its establishment as the Bureau for State Security (BOSS) (National Intelligence Service, 1994; Grundy, 1986).

The functions of the Bureau were to collect, evaluate, correlate and interpret national security intelligence for the purpose of defining and identifying any threat or potential threat to the security of the Republic; to prepare and interpret for the State Security Council a national intelligence estimate concerning the security of the Republic; to formulate, for the approval by the Council, a policy relating to national security intelligence; to coordinate the flow of intelligence between different government departments; and to make recommendations to the State Security Council on intelligence matters (Africa, 1992; Security Intelligence and State Security Council Act, 1972).

In order to facilitate the work of the country's first ever specialised intelligence service, the Security Services Special Account Act, 1969 (Act 81 of 1969) was passed. It made provision for the creation of an account for the control and utilisation of funds for services of a confidential nature and such expenses connected with the Bureau for State Security as deemed to be in the public interest. From the time of its establishment in 1969, throughout the seventies, BOSS achieved notoriety for its heavy-handed and intimidatory tactics. Even though it did not have powers of arrest, its crude and pervasive tactics – harassment of journalists and editors, blatant surveillance of political meetings, tapping of telephones and opening of mail of opponents of apartheid – won it widespread notoriety (Magubane, 2004).

The Bureau operated domestically and abroad. Geldenhuys (1984) observes that intelligence services operating secretly are often very influential structures, and in a short time this was the case with the Bureau, which came to play a significant role in South Africa's foreign relations. Van den Bergh was particularly active in Southern Africa as an emissary of Vorster in the détente era of the 1970s. He was, for example, instrumental in arranging the historic Victoria Falls summit between Vorster and President Kaunda of Zambia, in August 1975 (Geldehuys, 1984). Former officials of the Bureau admit that a large part of their operational effort was aimed at ending South Africa's isolation abroad, and to this end NIS operatives were deployed both inside the country and abroad. (National Intelligence Service, 1994).

Apart from the Bureau, the other elements of the statutory intelligence community and the state's secrecy system during this period were the Security Branch of the South African Police, and the Division of Military Intelligence (DMI) of the South African Defence Force (SADF). Both were involved in the political conflict in South Africa. The seventies saw the rise of worker and community resistance to apartheid, and a response of repression by the security forces. The role of the Security Branch of the SAP was to monitor resistance, and this was done through the coordination of an extensive network of informers in anti-apartheid groups, along with periodic detention without trial, harassment and surveillance of opponents of the state. Secret files were kept by the Security Branch on many of these opponents (Brogden & Shearing, 1993).

The most striking feature of the DMI was the extent to which it engaged both domestically and cross-territorially, in attacks on anti-apartheid activists, many of whom were in exile in

banned political organizations such as the ANC, the Pan Africanist Congress (PAC), Umkhonto we Sizwe and Poqo (the armed wings of these two movements), and the South African Communist Party (SACP). This was clearly in contrast to the conventional role of defence machinery, which was to defend a country's territorial integrity from foreign aggressors. In South Africa's case, the 'enemy' presented itself in the form of the frontline states of the Southern African region, which bore a three-fold brunt: economic domination by South Africa; the sponsorship of counterrevolutionary movements by Pretoria - Renamo in Mozambique and UNITA in Angola - and regular strikes on ANC bases on their own soil, often with civilians being casualties (Davidson, et al., 1976; Cawthra, 1986).

Apart from the Defence Act of 1957, which has already been described, other security legislation restricting access to information was in effect during this period. Considerable information about the role of the defence force was blacked out, so that even the press was unable to report on events of public interest. Gagging of the press was itself a secret, and the South African press was prohibited from reporting on South African Defence Force incursions into neighbouring territories such as Angola (Mathews, 1978).

Another significant statute restricting the disclosure of information was the Atomic Energy Act of 1967, which criminalised disclosure or unauthorised publication of information relating to source or nuclear materials, or research, invention or discoveries concerning nuclear or atomic energy. The receipt of such information communicated in breach of the law was also a crime, as was failure to protect such information once so communicated. A similar provision was contained in the Nuclear Installation Act of 1963 and regulations enacted under the Uranium Enrichment Act and 1970. Again, these provisions were as broad, if not broader, than the provisions under the Official Secrets Act, with the result that the reach of the law, extended,

> …outside the appropriate government departments or government created boards or corporations, to information in the hands of private bodies or citizens. It covers researchers in the field of nuclear science and even teachers who could breach the provisions of the act by discussion in the classroom or with colleagues.
>
> (Mathews 1978:148)

There was strict regulation of access to state records by members of the public, including researchers and the media, in this period. The Act which preceded the National Archives Act was the Archives Act of 1962. It gave the Director of the Archives significant powers over the management of official records. Among other powers and responsibilities: the Director had to prescribe conditions for the physical care of all records, their classification according to an approved system, conditions for accessing them, their inspection and ultimate disposal (Interview with Dr Graham Dominy, 2 September 2003).

In terms of the Archives Act 1962, records could be made available to the public after a period of fifty years had lapsed. Moreover, their legal disposal involved either a transfer to the Archives or destruction in terms of a disposal authority. Until 1979 a statutory body, the Archives Commission was responsible for authorising the destruction of records. In 1979, the Act was changed, giving the Director of Archives this power. Even though he was thus empowered, several departments made use of the ambiguous formulation in the law, to avoid their being subject to the disposal requirements of the Act (RSA, Truth and Reconciliation Commission Report, 1998).

Censorship of the media played a significant role in restricting access to information. The Publications Act of 1974 provided for the prohibition of the distribution, publication or exhibition of "undesirable" publications, films and entertainment, and powers were given to a committee to exercise judgment about what media fell within the scope of acceptable norms. The decisions of the committee were binding in criminal cases. According to the statutory definition, material was deemed to be undesirable if it was "prejudicial to the safety of the State, the general welfare or the peace and good order" (Mathews, 1978:151). Mathews (1978) further cites the example of the use of the Act to ban a 1976 a publication of the Christian Institute entitled *"South Africa - a Police state?",* because the publication listed the names of people held in detention under various security laws, described details of major political trials of the previous three years, and indicated the type of torture that had been used by the police.

Not only did apartheid legislation suppress the disclosure of information, it also infringed on personal liberties and privacy. Section 118A, inserted in the Post Office Act in 1972, gave the

Minister of Posts and Telecommunications, or a Minister who was a member of the State Security Council, or an officer delegated by the Minister, authority to direct that any particular postal article, telegram or communications by telephone, to or from any particular person, body or organisation, be intercepted for such periods deemed to be in the interests of the security of the Republic (Mathews, 1971).

1976 - 1990

In 1976, hundreds of youths left the country to take up arms against the apartheid government, following the Soweto uprisings against the introduction of Afrikaans as a medium of instruction in black schools. The unprecedented resistance of the period, and South Africa's consequent increasing international isolation, led its rulers to review their security strategy. The 1977 White Paper on Defence presented the role of the defence establishment as being to uphold the right of self-determination of the 'White Nation' (Cawthra, 1986; Grundy, 1986).

Co-option was a significant feature of the apartheid government's strategy of white domination. The intelligence services of the TBVC states – the "independent" Republics of Transkei, Venda, Bophutatswana and Ciskei, which on paper were constitutionally independent of South Africa, had powers to legislate on areas of service delivery governing their people's lives, thus giving rise to a myth of political independence (Bindman, 1988). In reality, the TBVC states were economically dependent on South Africa and regarded by the international community, including multilateral bodies such as the United Nations and the Organisation of African Unity (OAU) as a mere extension of the policy of apartheid. In addition, there existed another half dozen self-governing national territories or black "homelands" – rejected by the majority, and internationally unrecognized (Bindman, 1988). The self-governing territories attained their status in accordance with the Self Governing Territories Act, 1971, an Act passed by the country's white parliament, which provided that any legislative assembly established in terms of the Act, could make laws in a number of designated areas, including policing, but excluding intelligence. All six territories did indeed opt to establish their own police forces.

The intelligence services of the Transkei Intelligence Services, the Bophutatswana National Intelligence Service and the Venda National Intelligence Service, were modelled - in law at least – on the apartheid government's own National Intelligence Service, but staffed by "citizens" of the respective Bantustans. Like the mainstream white services, the TBVC services focused on frustrating the political opposition, by spying on members of the oppressed communities. The TBVC states' intelligence services received training and resources from the South Africans, and served the same end, namely to prevent the country from falling into the hands of the black, disenfranchised majority. In addition, the police forces of all these homelands served as an extension of the apartheid state's repressive machinery. For example, while it never developed a statutory intelligence service, the KwaZulu Police acted in collusion with warlords, certain chiefs and vigilante groups to quell political opposition to Buthelezi.

The "total strategy" introduced by the Defence White Paper of 1977 was intended to coordinate all aspects of national life – the military, economic, political, sociological, technological, ideological, psychological and cultural (Hansson, 1990). South African society became increasingly militarised in the 1970s and 1980s. Among the more notorious security institutions was the Civil Cooperation Bureau (CCB), an offshoot of the Special Forces, which was engaged in an extensive political assassinations campaign (Cawthra, 1986). At the height of apartheid in the seventies and eighties, security policy and strategy were coordinated at the national level by the State Security Council (SSC), a Cabinet committee chaired by the country's State President and consisting of Ministers responsible for the country's security services, in the main.

Significantly, the heads of the intelligence services also served on the SSC, giving them tremendous influence in national decision making. The State Security Council was established in terms of the Security Intelligence and State Security Council Act (No. 64 of 1972). Influential in national politics to the extent that the full Cabinet merely served to rubber-stamp decisions that had been taken there, the SSC introduced the National Security Management System (NSMS) in 1979, which sought to integrate the security and welfare aspects of a "total strategy", aimed at maintaining white political control (Cawthra, 1986; Grundy 1986). The rationale of this strategy of "winning hearts and minds" (WHAM) was that a governing power could defeat any revolutionary movement if it adopted the

revolutionary strategy and principles and applied them in reverse. The NSMS evolved over time to new forms of control over the growing national resistance and the failure of the government's reform. By the middle of the nineteen-eighties, state strategists began to describe South Africa as being involved in a low-intensity conflict around which the entire population, including black people at grassroots level, had to be mobilised (Hansson, 1990; Haysom, 1992).

Seegers (1990: 25) describes the contest for influence and control between elements of the security forces in the mid-1980s:

> Security intelligence was impeded by rivalry among the state security bodies and by a lack of up-to-date information about activities at the local level. The core problem seemed to be a gap between planning and execution. This context was ripe for the execution of a military solution that stressed coordination and efficiency…The office of Executive State President, instituted in the new constitution of 1983, was a ready basis for a more executive style of government. It was hardly surprising then, that power relations within the state were restructured towards an executive dominated by the military.

More legislation aimed at consolidating secrecy and state security was also passed during this time. The Secret Services Account Act, 1978 had provided for the establishment of an account for secret services; monies could be transferred by the Minister of Finance to the following accounts at the requests of the Ministers concerned: the Foreign Affairs Special Account established by the Foreign Affairs Special Account Act, 1967; the Security Services Special Account; the Special Defence Account, established by section 1 of the Defence Special Account Act, 1974; the Information Service of South Africa Special Account, established by the Information Service of South Africa Special Account Act, 1979 and the South African Police Special Account, established by section 1 of the South African Police Special Account Act, 1985.

The effect of the above-mentioned legislation was to tighten control over information and further restrict opposition to the policies of the government at the time. Moreover, the legislation in general was intrusive, giving the state an inordinate degree of control over the lives of the people. In addition, Protection of Information Act, 1984 was passed. It repealed the Official Secrets Act, 1956, the Official Secrets Amendment Act, 1956, section 27 C of the Police Act, 1958, sections 10, 11 and 12 of the General Law Amendment Act, 1969, and section 10 of the General Law Amendment Act, 1972.

The Protection of Information Act, 1982, strongly resembled its primary precursor, the Official Secrets Act. It too provided for the protection from disclosure of certain information. In terms of the Act, there was a prohibition on obtaining or disclosing secret information to any foreign state or agent of such a state. Such information includes information relating to any prohibited place or anything in any prohibited place or any armament; the defence of the Republic, any military matter, any security matter or the prevention or combating of terrorism; any other matter or article, and which a person knows or reasonably should know may directly or indirectly be of use to any foreign state or any hostile organisation, and which, for considerations of the security interests or other interests of the Republic, should not be disclosed to any foreign state or to any hostile organisation (RSA, Protection of Information Act, 1982)

There is a heavy onus on the individual to be able to distinguish those matters that may prejudice the interests of the state. The Act was clearly designed to ensure that access to information was denied, both to foreign states, and to opponents of apartheid. The emphasis was on the denial of access to information, and this created barriers to the public's right to information in order to play a meaningful role in public policy formulation. The Protection of Information Act is still in force today, and sits uneasily alongside the Promotion of Access to Information Act, 2000, as well as the National Archives Act, 1996.

A set of guidelines was introduced by Cabinet in 1978 to ensure uniform standards for the handling of classified information by public servants. In an interview, Commissioner Tertius Geldenhuys, Head of Legal Services in the South African Police Services (SAPS), described the background to the introduction of these guidelines. Prior to this time, the Official Secrets Act was in place, but there was no government regulation in place to ensure uniformity and

standardisation in the handling of sensitive government information. The responsibility for securing information therefore lay with individual Ministers and heads of department. The guidelines followed international norms and made provision for information to be classified at different levels of secrecy, and the procedures for their handling and safekeeping (Interview with Dr Tertius Geldenhuys, 7 October 2003).

According to the TRC Final Report (1998) the 1978 guidelines empowered department heads to authorise destruction. They ignored the provisions of the Archives Act, which gave the responsibility for the final custodianship of all records in the ambit of the State Archives. The guidelines issued by Cabinet did not outside explicitly state that the powers given to the Director of the State Archives in law were being replaced or retracted. But the weight of a Cabinet decision was sufficient to allow state departments to act without hindrance in the routine destruction of state records. This power was exercised routinely within the security establishment. The State Archives Service claimed to have become aware of the guidelines only during 1991 (RSA, Truth and Reconciliation Commission Report, 1998).

From 1983, the routine destruction of records was commonplace in the NIS, which worked from the premise that its records fell outside the ambit of the Archives Act. I interviewed Advocate Marius Ackerman, former State Law Advisor in the State President's office about the status of documents in the custody of the National Intelligence Service. He pointed out that:

> There was a difference of opinion between the State Archives and security departments on the meaning and effect of the Archives Act. The former were of the view that all state documentation eventually had to be under their control, while the latter held the view that "sensitive documentation" could never be submitted in that way because state security and especially the safety of individuals could be compromised.
>
> (Interview with Advocate Marius Ackerman, 3 August 2003.)

There are, in fact, very few publicly available records of the NIS's activities under apartheid, and this institutional memory is unlikely to be recovered. In testimony before the TRC, former officials of the NIS admitted that the organisation had destroyed approximately 44

tons of records in the months preceding the country's first democratic elections. A massive operation saw thousands of employees in the security services and even other government departments shredding and burning all evidence that could give the ANC-led government insight into the methods, informants, and operations of the apartheid intelligence structures. The TRC Final Report notes, however, that among the records of the former regime that could not be traced, were the records of the National Security Management System (NSMS), a substructure of the State Security Council (RSA, Truth and Reconciliation Commission Report, 1998).

The NSMS was disbanded in 1989 by the last State President to preside over apartheid, F.W. de Klerk, and the status of the SSC was reduced to that of an ordinary cabinet committee (Hansson, 1990). These developments took place at a time where there was not only unprecedented popular and international resistance to apartheid, but also growing schisms within the ruling party. After De Klerk's appointment, the military began to lose its predominant influence over political life in the country, though it still remained a significant factor throughout the events that were to unfold.

In summary, it can be argued that all above-mentioned components of the statutory intelligence community - the civilian National Intelligence Service and its predecessor, BOSS, the Security Branch of the South African Police, the Division Military Intelligence of the SADF, and the satellite intelligence services of the TBVC states - coalesced to ensure the maintenance of apartheid. This is not to deny that there were contradictions between these role-players from time to time, or even that apartheid was homogeneous and interest-free over the years. At times, the rivalry between military intelligence, the Security Branch and the NIS was quite stark. But collectively, these agencies wielded considerable power, as a result of the methods and access to information and the halls of authority that they wielded.

Concluding remarks

What this chapter has highlighted is that South Africa in its pre-1990 years was characterised by a closed and secretive form of government. Official secrecy and political exclusion worked hand in hand to marginalize the country's black majority and opponents of the racist government. Modelled on British legislation, South Africa from 1912 was subject to the

Official Secrets Act, which provided for severe mandatory penalties for disclosure of state secrets. Domestic foreign policy was driven by the need to resolve the "Native question", which was finally consolidated in 1948 through the ascent to power of the Afrikaner-dominated National Party. In subsequent years, much of the legislation aimed at consolidating white rule had the effect of silencing opposition and suppressing the basic human rights of individuals, such as freedom of speech, movement, and expression. As I have attempted to show in the literature review, in my discussion on international conventions, the denial of these freedoms is tantamount to the denial of access to information, in the broader sense.

The Official Secrets Act was replaced in 1984 by the Protection of Information Act, which, if read in conjunction with other legislation, reinforced the culture of penalties for the disclosure of secrets. Important issues of accountability, of who defines what is legitimately to be withheld as secret or confidential and what checks and balances exist over how officials exercise diligence in their management of information, continued to be ignored. This is not surprising, given that apartheid South Africa was facing an unprecedented crisis at the time.

The role of the State Archives Service in managing security records appears to have been ambiguous, and this ambiguity, it seems, was exploited considerably by the state security organ. A considerable amount of documentation was to be eliminated in the early nineties, in the months before the first democratic elections, effectively eliminating a considerable proportion of official memory.

In the periods that I have reviewed, security policy and secrecy measures of successive white minority governments have been aimed at consolidating white rule, while at the same time, influencing international opinion in favour of South Africa's domestic policies. In the apartheid era, South Africa had neither a specific system for the declassification of security-sensitive information, nor a regime of access to information legislation. Volume One of the Truth and Reconciliation Commission Final Report, in reporting on and assessing the implications of the destruction of records, points out that the fundamental guideline governing public access to state records during the apartheid period was provided in the Archives Act of 1962, which established that access was a privilege to be granted by bureaucrats.

The apartheid inheritance included a classification system which was contained in the Cabinet guidelines for the protection of classified information. The range of classification designations most commonly utilised by officialdom were "Top Secret", "Secret", "Confidential" and "Restricted". These designations were captured in a Cabinet guideline document entitled the Minimum Information Security Standards (MISS), and all state departments were expected to comply with the stipulations it contained. The guidelines do not cover the matter of who the authority to classify information rests with, how that authority is derived, and the conditions under which information may be reclassified.

Secrecy in pre-1990 South Africa was pervasive. It is impossible to divorce it from its political context, the effect of which was to cause much suffering to many people. The transition to a new political dispensation was characterised by the transformation of many institutions, including the intelligence services. This is the subject of the next chapter, which interrogates how fundamental this transformation has been, and whether the old patterns of secrecy have merely persisted.

CHAPTER FIVE

THE TRANSITION TO DEMOCRACY, AND ITS IMPLICATIONS FOR INTELLIGENCE ACCOUNTABILITY AND TRANSPARENCY

Introduction

In the previous chapter, I traced the history of secrecy in South Africa under minority rule. The research showed that secrecy provided a veil for the unaccountable and draconian conduct on the part of the security and intelligence services. This chapter analyses the conditions under which the post-apartheid civilian intelligence services came into existence, and how these have influenced the degree of public accountability of the services. My contention is that significant elements of the secrecy dispensation were carried into the transition. This was to impact on the management of information from the early 1990s until the new intelligence services were launched. This chapter analyses this claim, recognizing the critical role that the outcome of the negotiations for a framework for a democratic political dispensation played in mitigating the effects of previously unaccountable security and intelligence services. It therefore explores the legal framework and mechanisms for oversight of the intelligence dispensation during the negotiations for a new political dispensation in the early 1990s, during the period of the transitional authority under the interim Constitution of 1993, and finally, under the post-apartheid Constitution of 1996, and the effect of these mechanisms on broadening access to information about the intelligence services.

The context of negotiations for changes in the intelligence services

The mid-1980s to early 1990s, the backdrop to secret talks between senior ANC leaders and South African government officials in remote overseas venues, was an exceptionally violent period in South Africa's history. The United Democratic Front (UDF), a broad front of extra-parliamentary organisations had been launched in 1983, in a show of rejection of reformist moves, including the racially based tri-cameral parliament. The response to protests was a

show of force by the security forces and the South African state: detentions without trial, prosecutions and imprisonment under anti-terrorism and internal security legislation, political assassinations by apartheid hit squads, and security force instigation of "black-on-black violence" were the background against which very tentative and fragile overtures were made to explore negotiations between Pretoria and the exiled ANC (Collinge, 1992).

At the end of the 1980's, the government under P.W. Botha challenged the ANC to renounce violence if it was serious about negotiations, whilst the ANC, retorting that it was the government that should do so, encouraged its followers to pursue the armed struggle, mass action, and the international isolation of the South African government. The government's public posture changed remarkably after F.W de Klerk took the reigns of government in 1989.

De Klerk's lifting of the ban on the ANC, the PAC, the Communist Party and other proscribed organisations took observers, including the ANC, by surprise. It was followed swiftly by the release of Nelson Mandela and other high profile political prisoners from prison. These conditions led to the return of leaders of the exiled ANC to the country, to pave the way for negotiations (Haysom, 1992). The government and ANC signed the historic Groote Schuur Minute in May 1990, expressing "a common commitment towards the resolution of the existing climate of violence and intimidation from whatever quarter, as well as a commitment to stability and to a peaceful process of negotiations" (ISSUP 1992:17) The Minute paved the way for the adoption later that year of the Pretoria Minute signed between the parties in August 1990, reiterating their commitment to the Groote Schuur Minute.

Within government, a change in the philosophy and official discourse around security began to take hold in the early nineties. At a meeting of the country's top 500 police officers shortly before the unbanning of the ANC, De Klerk attempted to impress upon them their new responsibilities, and urged them to leave politics to the politicians (Nathan & Phillips, 1992).

From February 1990, following the unbanning of the ANC, political parties and organizations across the spectrum in South Africa began to give urgent attention to the processes of policy formulation across a broad spectrum of areas. In June 1991, the ANC held a major policy conference, prior to which draft policy resolutions were circulated to the organization's

branches. Meanwhile, the implementation of the Groote Schuur and Pretoria Minutes, particularly the return of exiles and a concomitant amnesty process, the release of political prisoners, and measures to contain the political violence still raging across the country, proceeded with difficulty. Accusations and counter-accusations about the each other's actual intentions flew between the government and the ANC. By this stage some 10 00 people had lost their lives in political violence since 1986, and over 30 000 had been displaced (Haysom, 1992). Notwithstanding their brief to stay out of politics, public confidence in the ability of the security forces to contain the violence was exceedingly low, and the ANC threatened to suspend negotiations with the government in April 1991. The stop-start process continued for some months, but agreement was finally reached by the government and other political parties and organizations that multi-party to discuss a future inclusive dispensation could begin. This was to take place at the Conference for a Democratic South Africa (CODESA) (Friedman, 1993).

CODESA's first meeting, held in December 1991, provided a platform for the parties to express their intent towards a negotiated political settlement. But the major effort was to happen later in the five working groups whose establishment the forum endorsed. The working groups were to consider proposals for the following: a climate for free political activity, constitutional principles to be included in a new constitution and the constitution-making forum; interim government/transitional authority/transitional arrangements; the future of the TBVC states; and time frames and modes of implementation of CODESA agreements (Haysom, 1992). Whilst they initially were not happy with the proposal, the government agreed that the decisions taken at CODESA were binding, after it was accepted that such decisions would require "sufficient consensuses" among participants. This formulation effectively meant that both the government and the ANC would have to be in agreement if the process was to move forward.

The discussions in the working groups were to continue over the next year, and CODESA convened again in May 1992, after each of the working groups, made up of representatives of the political parties, had held several meetings to discuss their briefs. CODESA 2, however, broke down because important debating points relating to the constitution-making process mainly had not been finalised. After this, there was a process of diplomatic talks between senior officials of the ANC and government aimed at getting the talks back on track.

A volatile political climate did not lend itself to the resolution of differences but, by this stage, both the government and ANC realized that they were so deeply embroiled in the process that they dare not let it fail (Friedman, 1993). This led to the signing of a Record of Understanding between the government and ANC in September 1992, which entailed agreement that remaining political prisoners would be released, that certain hostels would be fenced in, a prohibition on the carrying of dangerous weapons, and consensus that the elected constitution-making body could have one or two chambers, a fixed time frame and adequate deadlock-breaking mechanisms.

Whilst the negotiations took place in the highly politicized context in which a broad front of opposition players were rallied behind the ANC, the citizens of the country made limited inputs in the formal processes of negotiations. On the part of the ANC, consultative meetings with other organizations, including its alliance partners, the South African Communist Party and the Congress of South African Trade Unions, were one form of broadening participation. Feedback to its structures and public meetings were another vehicle but, by and large, it was the leadership elements within the party that determined overall organisational policy. There were parallels to this approach in government, which made use of its access to the levers of state power to call a referendum in February 1992, to seek endorsement for the direction it was pursuing in the adoption of an interim Constitution (Friedman, 1993).

The management of intelligence information during the negotiations phase (1990 -1993)

The transition to a new intelligence dispensation was part of a more generalised process of security sector transformation that had its genesis in the negotiations for a new political dispensation, notably in Working Group One at CODESA. Working Group One, charged with making recommendations on the creation of a climate for free and fair political activity subdivided into three sub-working groups, to address a wide range of concerns. These concerns included the return of exiles and the release of political prisoners, the repeal of security legislation and other repressive laws, and the future of the security forces (Friedman, 1993). The final report of Working Group One included the following recommendations: that the security forces be subject to the supremacy of the Constitution, that they be politically non-partisan; that they respect human rights, non-racialism and democracy; and that they

strive to be representative of the society as a whole. In Working Group Three, agreement was reached that the security forces be placed under the control of the interim government structures.

At this time, the Constitution in place was that which had been adopted in 1983, making provision for the racially-based tri-cameral parliament. It made no provision for access to information. However, a liberalisation of the political space was emerging, making it possible for the media to report on significant national events. Security legislation such as the Internal Security Act, the Riotous Assemblies Act and the Terrorism Act, however, remained in place. Intelligence services were managed as separate entities, and the intelligence information of the state was proprietary.

The direct role of intelligence structures both in the negotiations process and in the creation of a new intelligence dispensation was significant and officials on both sides were drawn into the process to map out a future intelligence dispensation (O'Brien, 1996). The ANC's Department of Intelligence and Security (DIS) had been formed in 1969, following a decision by the movement's leadership that it needed a body that could counter attempts to crush its military wing, Umkhonto we Sizwe.

Nhlanhla (1992) had earlier argued that the apartheid security services were pervaded by a militaristic and racist culture where the interests served were those of the ruling Nationalist government and not those of the people as a whole. Moreover, they existed in a culture of secrecy and lack of transparency and accountability to the public. Because of these conditions, they were able to resort to detention and torture, assassinations and kidnappings, in pursuit of the interests of state security. This was an inward-focused approach where the greatest threat to national security was seen to come from fellow South Africans engaged in the liberation struggle. Nhlanhla, at the time the African National Congress's head of intelligence, argued that intelligence services had a role to play in the affairs of state, and that,

> the world over, intelligence activity is, by its very nature, characterized by secrecy and stealth…an understandable and often necessary feature, as the defence of national security often

> requires the withholding of information that might be used against a country by would-be aggressors.
>
> Nhlanhla (1992:70)

The National Intelligence Service (NIS) also proclaimed the success of its existence, which roughly equaled that of the ANC in length. Daniel Barnard, a former head of the NIS, argued that during his term of office in the NIS, its role was not limited to supplying security intelligence; it also laid a foundation for the country's future by facilitating negotiations between the apartheid government and its opponents. Barnard stressed that the NIS could fulfill this function because it was "schooled in the age old universal fundamentals of the intelligence profession, it seeks the truth and it undauntedly conveys it to the government" (National Intelligence Service, 1994).

From early in the 1990s, the newly appointed NIS Director-General, Mike Louw, spoke of the need for greater openness in intelligence matters and promised greater transparency in the part of his agency (*Sunday Times*, 23 February 1992). Under then President De Klerk, the portfolio of intelligence was shifted from the exclusive control of the State President's office, and handed to the cabinet minister responsible for the Justice Portfolio. The general framework within which ANC security policy was couched was significant for the values it espoused, and accorded strongly with those being espoused in liberal democracies in the post-Cold War era. Regarding intelligence, the following resolution was adopted by the ANC at its June 1991 policy conference, a position that was to become the basis for the ANC input in the negotiations process:

> The national intelligence agency will be responsible for gathering, collating and evaluating strategic information that pertains to the security of the state and the citizenry;
>
> The national intelligence agency shall respect the rights of all South Africans to engage in lawful political activity;
>
> Intelligence activities shall be regulated by relevant legislation, the Bill of Rights, the Constitution and an appropriate Code of Conduct;
>
> All intelligence institutions will be accountable to parliament and subject to parliamentary oversight;

> The public shall have the right to information gathered by any intelligence agency subject to the limitations of classification consistent with an open and democratic South Africa;
> The national intelligence agency shall be politically non-partisan; and
> The national intelligence agency shall guard the ideals of democracy, non-racialism, non-sexism, national unity and reconciliation, and act in a non-discriminatory way.
>
> (African National Congress, 1991)

Senior ANC members say that the ruling government had at first resisted the idea of negotiating a new intelligence dispensation, on the grounds that intelligence issues could not be discussed in open political forums. They offered, it is said, to simply absorb members of the liberation movement's and the TBVC states' intelligence structure, into the NIS. This maneouvre was rejected by the ANC, and the political players, including the intelligence components, went on to negotiate a new intelligence dispensation (Interview with Moe Shaik, 17 October 2003).

Even as CODESA met, with the talks breaking down at times over differences between the ANC and the National Party, the DIS and NIS were determined not to allow these disruptions to derail their efforts to find common ground. In this regard, a series of bilateral meetings was held between DIS and the NIS, resulting in agreements on a set of basic principles to guide intelligence work in the new dispensation, the need for the establishment of a sub-council on intelligence under the authority of the impending Transitional Executive Council, and the terms of reference of such a sub-council (Interview with Moe Shaik, 17 October 2003).

It was during this period that the mass destruction of documents relating to the apartheid security establishment gained intensity. The previous chapter has already examined the implications of the state's interpretation that "sensitive records" fell outside the ambit of the Archives Act. Even though the ANC Commission on Museums, Monuments and Heraldry proposed a moratorium on the destruction of state records in 1992, it was powerless to see this recommendation through (Interview with Verne Harris, 1 September 2003). Instead, government departments were authorized by Cabinet to destroy records containing sensitive information. This followed the decision of the Minister of Justice and National Intelligence to

authorize the destruction by the NIS of financial records outside of the parameters required by the Treasury, at the end of the Kahn Commission of Inquiry into Special Projects.

The TRC Report on the destruction of state records suggests how devastating the impact was on the actions and administrative decisions relating to records, made by the state during the early days of negotiations. The report states that over a six to eight month period in 1993, NIS headquarters alone destroyed approximately 44 tons of paper-based and microfilm records. All state departments were instructed to transfer all documents that had originated as State Security Council Secretariat records, to the NIS, which was the custodian at the time of the State Security Council. For this massive destruction exercise, the Pretoria-based Iron and Steel Corporation (ISCOR) furnace, among others, was used. According to the report, much of the destruction took place outside the parameters of the guidelines for the disposal of records, and was intended to obliterate any trace of operations, lists of sources or other compromising details that the security establishment might have to explain in a future setting. As a result a massive vacuum in the corporate memory of the NIS, along with that of other security institutions, was created. (RSA, Truth and Reconciliation Commission Report, 1998).

The ANC and other parties were powerless and probably unaware of the extent of the destruction of records in this early period. The government had only just lifted its restrictions on the movement, which along with that of extra-parliamentary groups was the subject of intense scrutiny by the security forces and the intelligence services. The fact that the two sides sat across the table in 'talks about talks' did not mean that either was prepared to share secrets, since their most potent secrets were about each other.

The management of intelligence information under the Transitional Executive Council (June 1993 – April 1994)

The South African political transition has raised questions about the status, legitimacy and ownership of intelligence information in the process of moving from authoritarian to democratic rule, and in the earliest stages of consolidating democracy. This was undoubtedly an area of contestation in the transition period. My analysis of policy, provided below, legislative and administrative instruments that were established or enforced in that period

suggests an ambiguous impact on access to and control over security information of the apartheid-era security institutions.

The Transitional Executive Council Act of 1993 gave expression to the arrangements provided for in the negotiations process. The country was to be co-governed by the Pretoria government and the ANC, whilst preparations were undertaken for democratic elections. Seven Sub-Councils provided for in the legislation were set up to facilitate this process. These were the Sub-Councils on Defence, Law and Order, Intelligence, Finance, the Status of Women, Foreign Affairs, and Regional and Local Government. The role of the sub-councils amounted to a form of multi-party scrutiny over the above-mentioned areas of governance. The function of the Sub-Council on Intelligence, spelt out in the legislation, was to adopt a set of basic principles on intelligence which could also serve as a basis for the creation of a national capability in a new democratic dispensation. It also had to formulate a code of conduct that would be binding on all members of all services during the period of transition and that would serve as a basis for an official code of conduct in a democratic South Africa (Transitional Executive Council Act, 1993).

Under the TEC, the intelligence services of the apartheid government were to remain intact, as were those of the TBVC states, and the liberation movements. The intelligence services continued to serve their principals with information during this critical period, but were bound by political agreement to begin crafting a single intelligence framework for the future. Unavoidably, the leaders of the intelligence structures were drawn into negotiating their common future.

The TEC Act also made provision for the establishment of a Joint Coordinating Intelligence Committee (JCIC) whose function was to provide to the TEC on a regular basis with intelligence estimates concerning the security situation in country in the run-up to the elections. The ANC had originally wanted all intelligence structures to report to the JCIC but backed down on this demand when the NIS insisted that all components should retain control of their day-to-day management processes. The JCIC comprised the heads of all the intelligence services and departments in the country drawn from the civilian service, the various police and military forces. The JCIC effectively managed the various intelligence services during this period of transition. In addition to providing the TEC with appropriate

intelligence, the JCIC played a crucial role in the run-up to the election by ensuring that all factors that could derail the process were duly monitored and reported on (Interview with Moe Shaik, 17 October 2003).

On completion of its task, the JCIC, on recommendation of the Sub-Council, established a forum, the Heads of Civilian Services - or HOCS as it was commonly called – comprising all the heads of the various civilian intelligence agencies, and a provisional national intelligence coordinating committee called NICOC. The task of HOCS was to ensure that the process initiated under the auspices of the sub-council in respect of the development of the future intelligence dispensation continue, whilst that of NICOC was to ensure that joint intelligence process also continued beyond the legal mandate of the TEC (Interview with Moe Shaik, 17 October 2003).

The fact that a degree of cooperation existed should not detract from the reality that the ANC operatives of the DIS and government officials in the NIS, were still on opposite sides of a political divide, in this critical period leading to the country's first democratic elections. In spite of the formal cooperation that had been introduced by the establishment of the TEC, secret information was a contested area in the political negotiations that preceded the country's first democratic elections. Both the National Party government and its political adversaries, particularly the ANC, were aware of the powerful leverage of institutions charged with intelligence responsibility and, throughout the period of negotiations, kept up their intelligence offensives with the view to understanding the activities and strategies of the other side. The existence of a legislative regime that criminalized disclosure of information, and internal regulations that bound members of the security services to secrecy, and the absence of available records make it almost impossible to assess objectively, the role of the NIS at the time.

The wide-ranging Protection of Information Act, 1982, and other draconian security legislation such as the Internal Security Act, 1982 remained in force during this time. A double-edged sword, security legislation at the time was probably as much directed against the liberation movement, with which government was busy negotiating a new political dispensation, as against the white-right wing, who were engaged in violent activities to derail the talks. The volatility of the situation should not be underestimated. There were strong

divisions in the apartheid security forces, with a number of members aligned with the extra-parliamentary white right wing. There was a real concern that information might be leaked to the right wing from inside the intelligence services, and a climate of mutual fear and distrust pervaded the ranks of the security forces (Haysom, 1992).

The management of intelligence information under the RSA Constitution of 1993 (the "Interim Constitution") from May 1994 – December 1994

In spite of ongoing political violence in the country, agreement was eventually reached on the contents of a new Constitution for South Africa. The Constitution of the Republic of South Africa, 1993 (Act 200 of 1993) came into effect on 27 April 1994, the date of the country's first democratic and non-racial elections. The 1993 Constitution contained a new feature in South African politics: an entrenched Bill of Rights, which guaranteed to the public a range of fundamental rights, including: the right to life; the right to equality before the law; the right to privacy; the right to freedom of expression, association, of movement, of access to the courts, to administrative justice; and most significantly, the public right of access to information (Mureinik, 1994).

On the last-mentioned right, the 1993 Constitution stated that,

> 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 protection of any of his or her rights.
>
> (Constitution of the RSA, 1993, section 23)

The period after the elections saw the intelligence services struggling to come to terms with their identity as defender of the new political order crafted by the country's democratically elected legislature. The broadened concept of security contained in the Interim Constitution was undermined in reality by the continuities in both the discourse and practices of security. A cogent example was expressed through the maintenance of some of the old traditions and practices of managing security information. A case in point was the continued destruction of

records until Cabinet declared a moratorium on destruction of records in 1996 (RSA, Truth and Reconciliation Commission Report, 1998).

The post-1994 period saw wide discretion given to intelligence officials in their determination of classification levels considered appropriate for information generated in the course of their work. The practice within the security organs was to shield from the public view, even those categories of information that did not pose any harm if they were disclosed. Within the ANC, the practice of holding secret files on the activities of government targets continued (Interview with Moe Shaik, 17 October 2003).

Without a reasonable degree of transparency, the public was obviously going to be at a loss as to what information it might request from the intelligence services. Within the statutory services – the NIS and the TBVC services - intelligence information and much other official documentation continued to be routinely classified as "Top Secret", "Secret", "Confidential" or "Restricted", depending on the perceived degree of harm to national security that disclosure of such information would cause. The criteria by which the state declared degrees of accessibility or non-accessibility to information it created or held could not be subject to scrutiny, because no oversight framework with which to do so existed.

By the time that the country's first democratic elections were held in April 1994, the intelligence components of the statutory and non-statutory forces, at least at leadership level, were already in deep discussion about their integration. After the elections, on the basis of the reports of the Sub-Council on Intelligence, further negotiations occurred at the bilateral level to develop the future intelligence dispensation. These discussions influenced the debate within the new democratic parliament. A White Paper on Intelligence and three Bills, namely the Intelligence Services Bill, the National Strategic Intelligence Bill and the Committee of Members of Parliament on and Inspector Generals of Intelligence Bill, were presented to the legislature for approval (Interview with Moe Shaik, 17 October 2003).

The White Paper on Intelligence, adopted by Parliament in 1994, warned against the intelligence services adopting a militaristic approach to security, as was the case under apartheid, when "emphasis was placed on the ability of the state to secure its physical survival, territorial integrity and independence, as well as its ability to maintain law and order

within its boundaries" (RSA, White Paper on Intelligence, 1994). It further signaled that "… the main threats to the well-being of individuals and the interests of nations across the world do not primarily come from a neighbouring army, but from other internal and external challenges such as economic collapse, overpopulation, mass migration, ethnic rivalry, political oppression, terrorism, crime and disease" (RSA, White Paper on Intelligence, 1994).

The following responsibilities for intelligence were incorporated into the new government's policy document, the White Paper on Intelligence which was adopted by Parliament in 1994: the safeguarding of the country's democratic Constitution; the upholding of the individual rights enunciated in the Constitution's Bill of Rights; the promotion of the interrelated elements of security, stability, cooperation and development, both within South Africa and in relation to Southern Africa; making an active contribution to global peace and other globally defined priorities for the well-being of humankind; the promotion of South Africa's ability to face foreign threats and to enhance its competitiveness in a dynamic world (Africa & Mlombile, 2001).

The intelligence services would be governed by the following principles, all in sharp contrast to the principles that appeared to govern intelligence under apartheid: the primary authority of the democratic institutions of society; subordination of the intelligence services to the rule of law; compliance of the intelligence services with democratic values such as the respect for human rights; political neutrality of the intelligence services; accountability and parliamentary oversight for the intelligence services; maintaining a fair balance between secrecy and transparency; separation of intelligence from policy-making; and an ethical code of conduct to govern the performance and activities of individual members of the intelligence services (RSA, White Paper on Intelligence, 1994)

The Intelligence Services Bill, 1994, proposed the amalgamation of the statutory and non-statutory intelligence services, into two civilian intelligence departments: a foreign intelligence department responsible for external collection of intelligence about threats emanating from abroad; and a domestic department focused on internal threats to security. The domestic department would also hold the counterintelligence mandate, and would ensure that foreign agents did not penetrate the South African intelligence machinery (Africa, 1994).

The second draft Bill, the National Strategic Intelligence Bill, 1994, made provision for a mechanism to coordinate and integrate the intelligence inputs from the two civilian departments with the inputs from the intelligence divisions of the South African Police Service and the South African National Defence Force, in order to advise the government on threats and potential threats to the security of the country and its citizens (Africa, 1994).

And the third draft Bill, the Committee of Members of Parliament on and Inspector- Generals of Intelligence Bill, 1994 made provision for a multi-party parliamentary oversight committee with powers that would allow it to receive reports, make recommendations, order investigations and conduct hearings on matters relating to intelligence and national security, as well as an Inspector General to investigate complaints about the intelligence services. The Committee would also prepare and submit reports to parliament on the performance of its duties and functions (Africa, 1994).

On the basis of the recommendations of Cabinet, the Minister of Justice presented the Bills to parliament for consideration. Members of HOCS and their legal advisors appeared before the select committees of both the National Assembly and the Senate. After much deliberation and debate, the Bills were recommended by the two select committees to Parliament for adoption (Interview with Moe Shaik, 17 October 2003).

In anticipation of the new legislation, HOCS tasked various sub-committees to embark on the process of the amalgamation of the various intelligence services. In this regard, the following joint special work groups were established to make recommendations of the structures, budget, assets and human resource policies of the to-be formed intelligence services. Based on the reports and recommendations of these subcommittees HOCS formed an Amalgamation Committee (AC) to coordinate and implement the establishment of the NIA and SASS. The Committee established a number of so-called Super Working Groups consisting of representatives of the statutory and non-statutory intelligence structures. The Super Working Groups were tasked with implementing the decisions and agreements of HOCS, focusing on the practicalities that would have to be addressed in the migration to the new intelligence services. These working groups were established on a full-time basis and their reports were processed by the Amalgamation Committee for consideration by HOCS for decision-making (Interview with Moe Shaik, 17 October 2003).

Some of the issues addressed by the Super Working Groups were staffing requirements of the planned intelligence agencies, practical steps towards the establishment of the proposed structural changes themselves, budgetary implications for 1995/1996 financial year, and the development and implementation of an orientation programme for all members of NIA and SASS. The working groups also identified the functions that were to be shared by both services and mechanisms to ensure appropriate distribution and management of such shared facilities (Interview with Moe Shaik, 17 October 2003).

The RSA Constitution, 1993 made no provision for the principles that would govern national security, as this was still under debate in the negotiations for the reconstitution of the security services. Neither did it make reference to the establishment of the intelligence services. The three Acts regulating the establishment and control of the intelligence community, particularly the civilian intelligence community, were passed, along with the White Paper on Intelligence, in the latter half of 1994, and the new intelligence dispensation effectively came into being on 1 January 1995.

Changes within the intelligence structures of the South African Police Service were also informed by the principled outcome of the negotiations process (Africa & Mlombile, 2001). Following 1994, the new non-racial government's policy agenda on law enforcement was shaped by two objectives: firstly, to rehabilitate the police to ensure that they served the communities of South Africa, rather than political ends, and secondly, to mobilize South African citizens to participate in the provision of safety and security (Africa & Mlombile, 2001). Among the oversight mechanism provided for in law, to ensure that the police kept to this brief were the establishment of an Independent Complaints Directorate, to receive complaints from the public about the conduct of the police, and a parliamentary oversight over the police.

Rauch (2004) describes the complexities in re-orientating the police, and the sometimes ambiguous signals sent out in the course of police reform. Africa and Mlombile (2001) recognized as significant that there had been a demilitarization of the rank structure of the South African Police Service and the appointment of appropriately skilled civilians into the Secretariat for Safety and Security, which was responsible for developing policy for the post-

apartheid Police Service. And in the new dispensation, the mandate of the Crime Intelligence Division of the South African Police Service is stipulated in the National Strategic Intelligence Act, 1994.

There were also significant changes in the governance and orientation of the armed forces in the post-apartheid period. These were the product of political negotiations about the integration of the liberation movements' armed formations and the apartheid military structures, and the role of the armed forces in a democracy. In the interests of entrenching democratic civil-military relations, the Defence Amendment Act, 1995 provided for a restructured Department of Defence comprised of the Defence Force (under the operational command of the chief of the armed forces), and a civilian Defence Secretariat, responsible for setting policy, and headed by the Secretary for Defence (Africa & Mlombile, 2001).

The RSA Constitution, 1996 was later to provide further context in which to locate the reform of the armed forces, and established a framework for civil-military relations in a democracy. The primary role of the defence force was defined as being to "defend and protect the Republic, its territorial integrity and its people in accordance with the Constitution and the principles of international law regulating the use of force" (RSA Constitution, 1996, section 200(2)). Like other sectors of the security services, the defence force was required to be politically non-partisan, to function within the ambit of the law, and subject to parliamentary oversight and accountability.

Defence Intelligence structures, falling under the operational command of the South African National Defence Force, and subject to the policy set by the Department of Defence, were also subject to the National Strategic Intelligence Act, 1994. The Act made a distinction between domestic military intelligence and foreign military intelligence, and stipulated the process to be followed in the collection of domestic military intelligence by the defence force, in support of the police and within the country. The rationale for these strict controls was to retain the professional status of the military and to avoid situations where it could become involved in domestic political conflict (Africa & Mlombile, 2001).

Lastly, the introduction of a statutory coordinating mechanism for the intelligence structures under the line-functional control of the Minister for Intelligence was another significant

development and was aimed at preempting inter-agency rivalry. In terms of the National Strategic Intelligence Act, 1994, a Coordinator for intelligence was responsible for coordinating the supply of intelligence by the different agencies to intelligence clients. The National Intelligence Coordinating Committee (NICOC) was made up primarily of the Coordinator and the heads of the intelligence services and structures. NICOC was required to provide strategic intelligence assessments including a "national intelligence estimate", which would provide an overall assessment of the threats to national security that the policy makers ought to heed over a forthcoming year.

The early experiences of the intelligence structures in the post 1994 period, indicate that there were difficulties in managing the shift in orientation. The democratic government inherited an as yet volatile political climate, and faced the task of neutralizing disaffected right-wing elements in society, some of whom had access to resources in the security services. In addition, violence in the townships persisted at such worrying levels, that the government was concerned that a "third force" - an organised body of individuals intent on undermining and destabilising the country - existed in the country's security forces (O'Brien, 1996).

The senior management appointed to head the intelligence services - was a reflection of the political compromises in the negotiations process, impacting sometimes on the way in which information was interpreted. The law stipulated that the civilian intelligence services would report to the President, initially through a Deputy Minister. In practice, the Deputy Minister reported through the Minister of Justice, who was also designated the Minister of Intelligence. The first Director-General of the NIA was Sizakele Sigxashe, a former senior leader of the ANC's DIS, whilst the first Director-General of the SASS was Mike Louw, who had been Director-General in the apartheid-era NIS. The chain of command in the SANDF was Joe Modise, a former ANC military commander as Minister of Defence, with Lieutenant-General Dirk Verbeek, a former South African Defence Force officer as Chief of Staff Intelligence. In the South African Police Service, Divisional Commissioner Grove in consultation with National Commissioner Fivaz, both apartheid-era policemen, reported to a Minister for Safety and Security – Sydney Mafumadi – with an ANC background (O'Brien, 1996).

Some of the political scandals that beset the intelligence services were the product of political differences at the top. This affected the quality of intelligence provided to government. One

of these incidents was the hand delivery of a classified intelligence report to President Mandela, by the Chief of Defence Intelligence. The report had bypassed the NOC structures and claimed that senior military officers with an ANC background were plotting a coup. A judicial team appointed to evaluate the report dismissed it as lacking credibility and the chief of Defence Intelligence was relieved of his post (Africa & Mlombile, 2001).

Africa and Mlombile (2001) argued that the South African experience of reforming the intelligence services demonstrated the need to reflect the envisaged ideal mission, orientation and structures of accountability of the intelligence services in law and policy. It also showed the need to act decisively in responding to abuse or violation of the law, in order to propagate the alternate culture. Further, it pointed to the need to comprehensively review internal procedures to ensure that they are consistent with the legal framework. It was critical for each service to have clear and auditable procedures for authorizing operations, to enable a minister to confirm the legality of a particular operation. Finally, the critical role of parliamentary oversight bodies in monitoring implementation of transformation in the services, was stressed.

Impact of the Constitution of the Republic of South Africa, 1996 on the intelligence services

Section 198 of the RSA Constitution, 1996 spelt out the principles of a new security dispensation which declared that the security services must be structured and regulated by national legislation. Further, the Constitution required that:

> The security services must act, and must teach and require their members to act, in accordance with the Constitution and the law, including customary international law and international agreements binding on the Republic.
>
> No member of a security service may obey a manifestly illegal order.
>
> Neither the security services, nor any of their members, may, in the performance of their functions-
>
> (a) prejudice a political party interest that is legitimate in terms of the Constitution; or

(b) further, in a partisan manner, any interest of a political party.

To give effect to the principles of transparency and accountability, multiparty parliamentary committees must have oversight of all security services in a manner determined by national legislation or the rules and orders of Parliament.

Constitution of the RSA, 1996, section 199

The Constitution, in section 210 spelt out principles for the functioning of the intelligence services:

National legislation must regulate the objects, powers and functions of the intelligence services, including any intelligence division of the defence force or police service, and must provide for-

(a) the co-ordination of all intelligence services; and

(b) civilian monitoring of the activities of those services by an Inspector appointed by the President, as head of the national executive, and approved by a resolution adopted by the National Assembly with a supporting vote of at least two-thirds of its members.

Constitution of the RSA, 1996, section 210

And through its Chapter 9, the Constitution introduced a number of constitutional instruments aimed at promoting transparency and good governance over the security organs of the state. Among the institutions underpinning democracy and whose establishment was provided for in Chapter 9 of the Constitution were the Public Protector; the Human Rights Commission; the Commission for Gender Equality; the Independent Electoral Commission; the Auditor-General; and the Commission for the Promotion and Protection of the Rights of Cultural, Religious and Linguistic Communities (RSA Constitution, 1996, section 181).

Most importantly, the Constitution 1996 confirmed the right of access to information in Chapter 2 (the Bill of Rights), by giving persons access to any information held by the state as well as any information that is held by another person. As in the case of the Interim Constitution of 1993, the rights in the Bill of Rights are subject to reasonable and justifiable limitation.

Parliamentary oversight and access to information

It has already been pointed out that in the sphere of intelligence, the Committee of Members of Parliament on and Inspector-Generals of Intelligence Bill, which was later renamed the Intelligence Services Control Act, 1994 (No. 40 of 1994) provided for the establishment of a Committee of members of Parliament on Intelligence, and inspectors-general, and had the effect of placing the intelligence services under considerable oversight.

The Act gave the parliamentary committee access to intelligence, information and documents in the possession or under the control of a service, to the extent that such access was necessary for the performance of its functions, and on condition that information and records were handled in accordance with the existing security regulations. The Act, however, drew a line when it came to the names or identities of service members, sources, or methods of intelligence gathering. The services were not obliged to disclose these details to the Committee. Moreover, members of the Committee were required to undergo a security clearance process, managed by the NIA. In actual fact, the Committee functions within the bounds of secrecy of the intelligence services, and has had to tread a fine balance of being publicly accountable, satisfying Parliament that the services have been operating within the framework of the law, and ensuring that their own impartiality has not been impaired.

From the beginning, the Committee attempted to rise to the challenges set out in law, yet was aware of its own shortcomings. In her 1997-1998 Annual Report to Parliament, the Committee chairperson, Ms Nosiviwe Mapisa-Nqakula, admitted that it lacked capacity to deal with all its functions. That notwithstanding, it did engage the services vigorously, and promised to report back on a number of issues that at the time were tarnishing public perception about the services. These issues included mistrust between former statutory and non-statutory intelligence members, a lack of discipline, and corruption in the ranks. The JSCI expressed concern about these perceptions and promised to report back to parliament on the results of their investigation into the state of affairs in the services (Annual Report of the JSCI, 1997).

Chairperson of the JSCI, Siyabonga Cwele, stressed that it was important to see the role of the JSCI in facilitating access to information about the intelligence services, in historical conext. Under apartheid, virtually all information about the security services, including maladministration, were deemed state secrets. Parliamentary oversight of the intelligence services was therefore an import gain in the new constitutional order, and could not be arbitrarily taken away from the people (Interview with Siyabonga Cwele, 11 August 2005).

Cwele acknowledged the importance of the principle of transparency, but admitted that the JSCI had not played a proactive role in building public awareness about the intelligence services. He also admitted that the JSCI needed to consider more carefully, the implications of transparency for access to information about the intelligence services, and address directly the question of what information should be classified in their inputs to Parliament and when engaging the services. To illustrate this point, he argued that whilst the legislation governing the intelligence services made provision for the classification of only identities of intelligence workers, methods of collection and sources of intelligence, the tendency in the intelligence services was to classify almost all their records, thus creating a wall of secrecy (Interview with Siyabonga Cwele).

He said that it was questionable whether sources of intelligence should ever be disclosed, stating that this might put at risk the individuals who had provided information to a ruling government. Cwele stated that this was as true for South Africa as for several former East European countries where records of the former intelligence services were thrown open to the public, with traumatic social effects in some cases.

Cwele argued that the oversight system in South Africa was still evolving, and that the JSCI had taken several years to become a smoothly functioning entity. There was a general feeling in the JSCI that in spite of its important role and status - the Chairperson had to be appointed by the President - it had not impacted significantly on Parliament. In fact, there was a worrying misconception in Parliament, he said, that the JSCI functioned to promote and protect the interests of the intelligence community This was an unfortunate perception that the Committee would have to actively correct, through being fair to the services when justified, but critical of their weaknesses and shortcomings when this was called for (Interview with Siyabonga Cwele, 11 August 2005).

Political party representation in the JSCI is proportional, with the result that the ANC held the majority of places, with several of the smaller opportunities enjoying only limited representation. Cwele did not consider this a deterrent to a vigorous oversight role being played by the Committee; if anything, he argued, the bolder and more assertive questions tended to come from the opposition parties, who were never victimized for their rigour (Interview with Siyabonga Cwele, 11 August 2005).

Finally, Cwele warned that there was a disturbing trend, internationally, of intelligence services wanting excessive powers, including a right of secrecy, in the aftermath of the 9/11 attacks on the USA. He stated that these could pose major setbacks to democratic gains, and pointed that this matter was being vigorously debated among oversight structures the world over. Under these conditions, and if legislation to counter terrorism were passed, the JSCI would have to be more vigilant than ever in monitoring the services for compliance with the constitutional provisions that require the dignity of all persons to be upheld. Strengthening the capacity of the Inspector-General would be an important measure under these conditions he argued (Interview with Siyabonga Cwele, 11 August 2005).

The role of the Inspector -General of Intelligence

To extend the oversight function, the Intelligence Services Control Act, 1994 also made provision for the appointment of an Inspector-General or Inspectors-General with the responsibilities to monitor compliance by the services with their own policies, review the activities of the services, and perform all functions designated by the Minister concerned.
The Inspector-General had to be nominated by the oversight committee, and had to be approved by a joint sitting of both Houses of Parliament with a 75 percent majority. Among the reports that the Inspector-General was expected to compile for the Minister was one that recorded any unlawful activities or significant intelligence failures reported by the heads of the intelligence services.

Even though the function has existed in law since 1995, there was a slow start to the appointment of an Inspector-General for Intelligence South Africa. Dr Faizel Randera was appointed as Inspector-General in 2000, four years after Advocate Louis Skweyiya resigned

from this office after a brief tenure (Netshitenzhe, 2005). Randera's tenure was also relatively short, and he resigned in 2002 for personal reasons. To ensure that the office of the Inspector-General continued to function, the then Minister, Lindiwe Sisulu, appointed a Chief Operating Officer. The primary functions of this incumbent were day-to-day administration, investigations, research and review. The post of Inspector-General was filled again with the appointment of Zolile Ngcakani in 2003. With even more access to information than the JSCI, the Inspector-General has virtually unfettered access to information held by the services, in the course of fulfilling his or her functions.

Ngcakani acknowledged the critical role of the intelligence services in gathering information using secret methods and sources. Oversight structures such as the JSCI and his office were critical institutions in a democracy because they served to keep the intelligence services in check. However, he remarked that in his experience, he had found that the intelligence services tended to overclassify information and records, going far beyond the legal requirement of classifying methods, sources and identities of intelligence and counterintelligence operatives This was the result of the apartheid legacy, and was not in keeping with the principle of transparent and open governance on which the new political dispensation had been founded. Policy makers needed to consider whether there was need for such extensive secrecy about intelligence given that only about five percent on intelligence reports were informed by secret information. (Interview with Zolile Ngcakani, 3 August 2005).

Ngcakani stated that Cabinet was setting a good example in transparency, by releasing to the public details of the issues it had debated and taken decisions on, after every Cabinet meeting. He suggested that Cabinet should consider declassifying Cabinet memoranda, once resolutions had been passed on their substance (Interview with Zolile Ngcakani, 3 August 2005).

The role of the Auditor-General

A notable feature of the intelligence dispensation under apartheid was the extent to which the laws of the country made possible their comprehensive and secretive funding. The Security Services Special Account Act, 1969 provided for the establishment of a Security Services

Special Account. The account was to be utilized for services of a confidential nature and such expenses connected with the Bureau for State Security as deemed to be in the public interest.

Another piece of legislation, the Secret Services Account Act, 1978 provided for the establishment of an account for secret services. From it, money could be transferred by the Minister of Finance to the following accounts at the request of the Ministers concerned: the Foreign Affairs Special Account Act, 1967; the Security Services Special Account mentioned above; the Special Defence Account, established by the Defence Special Account Act, 1974; the Information Service of South Africa Special Account, established by the Information Service of South Africa Special Account Act,1979; and the South African Police Special Account, established by the South African Police Special Account Act, 1985. In all cases the Acts made provision for the funds to be disbursed in respect of confidential projects to be approved by the respective Ministers (Interview with Wallie van Heerden, 21 October 2003).

These laws suggested, on the one hand, executive responsibility for special projects of a secret nature. Parliament, however, had very little knowledge of the nature of the secret projects. It took, for example, the Harms Commission in 1977 to reveal that the security forces were in fact instrumental in political violence, through measures such as the establishment of death squads. And in 1999 the Erasmus Commission uncovered over 150 secret projects that had been conducted under the auspices of the Minister of the Interior, the Department of Information and the Bureau for State Security. All the projects, which included secret funding of some sections of the media for propaganda purposes, received state funding.

Against this background, financial accountability was to be a major concern under the new intelligence dispensation. In his address to Senate on the reading of the State Expenditure Budget on 12 May 1996, the Deputy Minister for Intelligence, Mr Joe Nhlanhla, identified the key elements of the government's financial planning approach: an overall reduction of the budget deficit and the level of government dissaving; reprioritisng government expenditure to meet the needs of the new South Africa; providing a stable and competitive environment, for growth and development and avoiding permanent increases in the overall tax burden; and managing state department budgets downward (RSA, Hansard, 12 May 1996).

Some insight is gained into the financial accountability of the services through a study of annual reports of the Auditor-General. The RSA Constitution, 1996 established the role of the Auditor General as being to audit and report on the accounts, financial statements and financial management of all national and provincial departments, municipalities and other institutions required by national or provincial law to be thus audited, and report to any legislature that has a direct interest in the findings. The Constitution very explicitly requires that all reports of the Auditor-General must be made public, in line with the constitutional principle of transparency.

For 1996-1997, the Auditor-General reported that although the financial statements were not being published for "strategic and security reasons", they were, in his opinion, a fair reflection of the financial position of the institutions concerned. Nevertheless, the following observations were among those made at the time by the Auditor-General about the financial statements and accounting practices of the intelligence services, many of them legacy issues from the apartheid era: the need for improved control measures over the payment of human sources; the civilian intelligence services' failure to compile an assets register; a lack of financial controls in the amalgamation of the TBVC states' security machinery into the national police service and the intelligence agencies; and the lack of an appointment of an Inspector-General, and the resultant fruitless expenditure (RSA, Report of the Auditor-General 1996/1997on the Audited Financial Statements of the Intelligence Services).

The same concerns were repeated in the 1997/1998 Report of the Auditor-General, and in the next. Although the Auditor-General reports indicated slow progress in attending to some of the concerns raised, the relationship between that Office and the respective departments was dynamic and revealed, at least, a sense of accountability on the part of the services. The concerns about financial management were not confined to the intelligence services. Many departments attracted negative audit reports in the early post-apartheid years, at once an indication of the legacy that they were adopting, as well as the lack of managerial experience on the part of many of those newly elected into office.

The Public Finance Management Act of 1999 (the PFMA) sought to ensure greater financial accountability and responsibility on the part of heads of departments. It accorded to them more flexibility in the achievement of objectives, whilst making them criminally liable in

case of the mismanagement of state resources. As national departments, the intelligence services were fully bound to comply with the provisions of the Public Finance Management Act, 1999 which prescribed a uniform, outcomes-driven and transparent approach to financial management in the public sector (Interview with Dennis Dlomo, 26 August 2003).

One concern, sometimes expressed from within the intelligence services, is whether disclosure of the intelligence budget, and the processes by which it is determined, could compromise the functioning of the intelligence services in their task of identifying threats to national security (Interview with Billy Masetlha, NIA Director General, 4 August 2005). Additionally, there is the question of whether adherence by the intelligence services to the statutory and regulatory processes of public financial management have similarly unintended consequences. These questions are all the more pertinent in the legislative context of the Promotion of Access to Information Act, 2000.

The PFMA attempted to ensure open and transparent budgetary processes, with a minister allocated clear responsibility for financial management. On the other hand, the intelligence laws made provision for operational secrecy in the intelligence services' execution of their mandates, and gave the minister responsible for the services the function of doing everything in his or her power to facilitate the work of the services (Interview with Dennis Dlomo, 26 August 2003).

The newly constituted intelligence services along with their counterpart structures in the SAPS and SANDF were not immune to the problems being experienced by other government departments. While there was broad agreement on what was desirable at the leadership level, making the new structures effective and rallying all members behind the new mission and priorities was a daunting challenge. Differences in levels of training and orientation, the mere physical relocation of many members and adjustment to new work conditions, and the legacy of the apartheid era, including involvement by the security forces in the violence prior to 1994, were bound to be felt.

Concluding remarks

To comprehend the management of intelligence information in the transition, one must understand the extent of repression out of which the negotiations emerged. When President F.W. de Klerk announced his dramatic reforms in 1990, thousands had already died in political violence, with the security forces not only ineffectual in turning the tide, but as was proven in subsequent investigations, instrumental in fomenting the violence.

The entrenchment of democratic principles arising out of the negotiations in legislation creating a Transitional Authority, the Constitutions of 1993 and 1996, and the enabling legislation establishing the intelligence dispensation, created the basis for a new culture of accountability and transparency over intelligence. The new services faced many challenges but oversight bodies appeared to be satisfied with their performance in the first five years.

Even though the intelligence services operated in terms of new legislation and repealed in entirety the old legislation, there were significant continuities with the old. In the HOCS phase, agreement was reached that the administrative systems of the NIS as well as their regulations would be initially used, and then revised within a short period of time. In reality, the review happened very slowly, and much later than anticipated, and the new services inherited and came to operate in terms of the arcane regulations and systems of the old order.

In addition, the introduction of a constitutional right of access to information rested uneasily with laws and administrative instruments designed to protect classified information. These laws and instruments were vestiges of the apartheid era and included the Protection of Information Act, 1984, and the Minimum Information Security Guidelines, the latter giving public official powers to restrict access to information.

On the other hand, there were substantial features of the new dispensation that were positive. Oversight structures such as the JSCI and Auditor-General were able to bring to the attention of the public both the strengths and weaknesses of the intelligence services. There was improved accountability of the responsible Minister in parliament, and the services were, for the first time ever, united about the nature of the enemy the country faced.

It must be said that whilst the process of restructuring the intelligence services was fairly comprehensive, it was not without weaknesses and problems. Nowhere was this more instructive than in the Janus-like legislative and regulatory dispensation under which the intelligence services function: the situation has simultaneously encouraged disclosure and openness on the one hand, and extended or tolerated significant withholding of classified information on the other.

The transition to a post-apartheid intelligence dispensation had a shaky start, but was rooted in strong principles of accountability and relative transparency. Criticism of the services was robust because they could be called to account by the Executive, the press and other actors in society. In South Africa, decades of the abuse of information as a source of power had discredited the intelligence profession. Even though the existing services were established in terms of new legislation, the legacy was difficult to shake off. The situation was not helped by the secrecy that surrounds the work of intelligence services.

CHAPTER SIX

IMPLICATIONS OF THE PROMOTION OF ACCESS TO INFORMATION ACT, 2000 FOR THE SOUTH AFRICAN INTELLIGENCE SERVICES

Introduction

This chapter outlines the evolution, aims and content of the Promotion of Access to Information Act, 2000 (PAIA), and assesses its implications for the civilian intelligence services of South Africa. It also analyses the policy and legislative context in which the PAIA has come into effect, and the challenges posed by these conditions for the services in making publicly justifiable choices around transparency and secrecy. And finally, it considers the experience of the USA, Canada and India (all countries with freedom of information legislation), assessing the impact of such legislation on the security and intelligence services of those countries.

My objective in this chapter is to assess the contention that the legislative and regulatory context in which the intelligence services function, is contradictory and creates the potential for ambivalence about implementation by various stakeholders. Currie and Klaaren (2002) have argued that the Protection of Information Act, 1982, is in fact unconstitutional, because it contradicts the provisions of the PAIA. I therefore assess the extent to which the PAIA recognises the need for secrecy, and explore whether secrecy and openness can be reconciled in a democracy.

The policy and legislative context of the PAIA

There are several significant legislative provisions regulating disclosure and the withholding of information in South Africa. In this section, I highlight the main features of these instruments of law.

The Protection of Information Act

At the time that the intelligence services were established in 1995, the most prominent law addressing the protection of information relating to national security, was the Protection of Information Act, 1982. The import of this Act has already been described in the previous chapter. The Intelligence Services Act, 2000 having undergone several revisions since it was first adopted in 1994 (Act 38 of 1994) further provides for the protection of "classified information". Section 10(3) of the Intelligence Services Act requires the heads of the intelligence services and the CEO of the South African National Academy of Intelligence (SANAI), to issue functional directives for the protection of classified information, as well as physical security, computer security and computer security.

The Act further prescribes that both members and former members are prohibited from disclosing classified information or material entrusted to them by the Director-General, the CEO (of the SANAI) or a member, without the permission of the aforementioned. Criminal liability may result in the event of these restrictions being violated (for both categories of persons a fine may be imposed, and imprisonment of up to five years in the case of a member, or up to ten years in the case of a former member). The restriction on former members applies to "any information or material received by the member during, or subsequent to, the former member's employment or other service with the intelligence services or the Academy, as the case may be, that was marked as classified, or that the former member knew or ought to have known was classified" (Section 27(1) of the Intelligence Services Act, 2002).

The National Strategic Intelligence Act, 1994

Further to this, the National Strategic Intelligence Act (No.39 of 1994), makes provision for the national intelligence structures to conduct a security screening of a person who is employed by or is an applicant for employment by an organ of state, or is rendering or gives notice to render a service to an organ of state if in the course of the interaction, they will have access to classified information and intelligence in possession of the organ of state, or will have access to areas designated as national key points in terms of the National Key Points Act, 1980 (section 2A of the National Strategic Intelligence Act, 1994).

The Intelligence Services Oversight Act, 1994

The parliamentary oversight body for intelligence, the JSCI is sworn to secrecy and required to conduct its functions in a manner "consistent with the protection of national security" (Section 5(1), Intelligence Services Oversight Act, 1994). In addition, section 4.2(a) of the Act provides that the services shall not be obliged to disclose to the Committee, the name or identity of any person or body engaged in intelligence or counterintelligence activities, or any intelligence, information or document in a form which could reveal the identity of a source of information provided to the service under an express or implied assurance of confidentiality.

In addition, the services may not, in terms of this Act, disclose any intelligence or counterintelligence method employed by the Service if this could reveal the name or identity of a person or body engaged in intelligence or counterintelligence activities, or the identity of a source. Where there is a dispute about whether releasing information could compromise the identities of persons engaged in intelligence or counterintelligence work, or sources, or methods of collection, an adjudicating panel consisting of the Inspector-General, the chairperson of the JSCI, the head of the service in question, and the Minister responsible for that service, will evaluate the arguments and take a final decision on the matter (Section 4(2)(b), Intelligence Services Oversight Act).

The Constitution of the Republic of South Africa, 1996

The most significant statute impacting on secrecy in South Africa, is the Constitution of the Republic of South Africa, 1996. The Constitution in the Bill of Rights, introduced the right of access to information. In addition, the Constitution introduced a number of instruments aimed at promoting transparency and good governance over the security organs of the state. Finally, the Constitution spelt out principles to govern national security and the conduct of the security services in the Republic.

National Archives Act, 1996

In the same year the Constitution was adopted, another significant legislative development addressed the impunity with which intelligence organisations had been able to set about the

destruction of official records in the last years of apartheid. Thus new government moved to preserve and secure all public records for posterity by drastically revising the Act relating to state archive collections and repealing the preceding Act.

The National Archives Act, 1996 (No 43 of 1996) provides for the proper management and care of the records of governmental bodies, and the preservation and use of a national archival heritage. In contrast with the preceding Act, the Archives Act, 1962, and various amendments thereof, the Act places greater emphasis on the accessibility of government records to the public. Thus, the functions of the National Archives were to preserve public and non-public records with enduring value for use by the public and the State; to make such records accessible and promote their use by the public; and to promote an awareness of archives and records management, and encourage archival and records management activities.

The Act also makes provision for access to and use of records in the custody of the National Archives, the broad guideline being that any such public record shall be available for public access if a period of twenty years has lapsed since the end of the year in which the record came into existence. Intelligence records fall within the scope of the Archives, and their destruction is not possible without the express authority of the National Archivist. However, the Act is not without weaknesses, which may seriously impact on the effectiveness, and raise serious questions about the real balance of power between the national archives and the intelligence services.

Communications-related legislation

In 2002, as part of a broad initiative to build technological capacity the following Acts were passed the Regulation of Interception of Communications and Provision of Communications Related Information Act, the objectives of which were to regulate the interception of certain communications subject to authority been granted; to simultaneously prohibit unregulated service provision of telecommunications services that cannot be intercepted; to establish interception centres and the Office for Interception Centres; and to create penalties for non-compliance with the legislation.

The Electronic Security Communications (Pty) Ltd Act, 2002(the "COMSEC" Act), was the fourth significant legislative development in this period. The Act established the COMSEC, a state-owned enterprise, to protect and secure electronic communications of state structures against unauthorised access or other related technical or technical threats. All state organs would have to procure their electronic security products through COMSEC, which was to leverage its role in providing protection to critical electronic communications infrastructure, and coordinate research and development regarding any security risk to such infrastructure (Dlomo, 2004).

The Protection of Information Act, 1982 which had earlier been amended by the Intelligence Services Act, No. 38 of 1994, and the Justice Laws Rationalisation Act, No. 18 of 1996, was again amended by the Intelligence Services Act, No. 65 of 2002, the Electronic Communications Security (Pty) Ltd Act, No. 68 of 2002 and the General Intelligence laws Amendment Act, no. 52 of 2003. The effect of these latter amendments was to include in the definition of "security matter" protected by the Act, any matter dealt with by COMSEC, the Intelligence Services or the Academy as defined in the Intelligence Services Act, 2002 and the Office as defined in the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002. Protection was also afforded to information relating to the functions of these bodies, or the relationship existing between any persons and them (Protection of Information Act 1982, section 1). Whilst it at least acknowledges information arising out of the activities of the newer intelligence entities as security-related, the definition of a security matter is problematic because it is vague. Some observers argue that the PAIA appears to provide clearer definitions about security related information that may be withheld from public disclosure and could be considered as a starting point for legislation protecting state information (Currie & Klaaren, 2002).

Assessment of the post-apartheid legislative context for secrecy

A number of contradictions and apparent legal flaws may be observed in the provisions outlined above. The first is that the law does not define "classified information", except by implication. The categories of information that the JSCI is prohibited from having access to, as listed above, may be interpretation as one being included under the umbrella of classified

information, by virtue of the prohibitions on their disclosure. However, the instrument for determining what is to be "classified" is a Cabinet guideline, the Minimum Information Security Standards, which is enforced in government departments, particularly the intelligence structures. The contents of the Minimum Information Security Standards (MISS) are not in the public domain and there exist therefore no statutorily determined criteria for the classification of information or documents.

Restrictions are placed on the JSCI, but apart from the implied allusion that such information as described is to be treated as "secret, these restrictions cannot be extended to members of the public, for whom the Protection of Information Act, 1982 is the source of legal authority. This which tables an extensive list of categories of information that is "protected", and which if disclosed, could result in criminal liability of the offending parties. Significantly, the categories of information listed in the Protection of Information Act, do not make expressly cater for a prohibition of the disclosure of the identities of persons involved in intelligence and counterintelligence work, nor of sources, or of methods of collection. In an interview, Ackermann remarked that:

> unauthorized access to classified documents per se, is not an offence in terms of the Protection of Information Act; the prosecution will have to prove that the disclosures, which are said to be transgressions, have been harmful to the security of the state.
>
> (Interview with Marius Ackerman, 28 August 2003.)

Since the enactment of the new Constitution, there have been extensive legislative changes aimed at achieving alignment with the Constitution. I have already described the legislation framing the post-apartheid intelligence dispensation. The Intelligence Services Control Act, 1994 (No. 40 of 1994) provides for the establishment of a Committee of members of Parliament on Intelligence, and inspectors-general, and has the effect of placing the intelligence services under considerable oversight. In order to effect a "watchdog" role, this legislation gives the parliamentary committee access to information held by the intelligence services, subject to limitations formulated to ensure that their legitimate intelligence operations and identities of confidential sources are not compromised. Other institutions

facilitating access to information included an open parliamentary system, an open and independent judiciary, and freedom of the press.

In addition, provision is now made through the Promotion of Access to Information Act, for a set of grounds for refusal of access to information. The question that arises in view of the existence of all these beacons for secrecy and transparency, is: which of these have statutory force, and which have administrative legitimacy? And where it is apparent that seemingly contradictory elements of the law must be implemented, what are the considerations to be followed in the decisions of structures such as the intelligence services? To answer this question, requires a thorough analysis first of the PAIA, which is provided below.

Origins of the Promotion of Access to Information Act, 2000

The Constitution of the Republic of South Africa, 1996 (Act 108 of 1996) also confirmed the public right of access to information in Chapter 2 (the Bill of Rights), by giving persons access to "… any information held by the state" as well as "any information that is held by another person, and that is required for the exercise or protection of any rights"(section 32(1)). As in the case of the Interim Constitution of 1993, the rights in the Bill of Rights are subject to reasonable and justifiable limitation. Section 36 stipulates that the limitation must be:

> reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom taking into account all relevant factors including:
> a) the nature of the right;
> b) the importance of the purpose of the limitation;
> c) the nature and extent of the limitation;
> d) the relation between the limitation and its purpose; and
> e) less restrictive means to achieve the purpose.
>
> (RSA Constitution, 1996, section 36)

Section 32 of the Constitution stated that national legislation should be enacted to give effect to this right. It should be noted that the 1993 Constitution did not stipulate that an Act of Parliament should be enacted to give effect to the constitutional right of access to information, as the 1996 Constitution was later to (Interview with Empie van Schoor, 25

August 2005). However, in 1994, a Task Team was established in the office of the then Deputy President, Thabo Mbeki, to draft the legislation. The Task Team was convened by Advocate Mojanku Gumbi, assisted by Advocate Vincent Maleka, Professor Mandla Mchunu, Professor Etienne Mureinik and Advocate Empie van Schoor, a State Law Advisor. Mr Adriaan Nortje served as the secretariat to the Task Team. The Task Team had a broad brief: to draft a law that would cover the following aspects: access to information, access to meetings, and the protection of whistleblowers. In their early deliberations about the principles that should underlie the Act, the principle of maximum disclosure was paramount (Interview with Empie van Schoor, 25 August 2003).

According to van Schoor, the team studied the access to information of several countries including Australia, New Zealand, Ireland, the USA, Britain (in draft form), and India (also at a draft stage), and met regularly to discuss the draft. In a policy proposal document (19 January 1995), the Task Team said that this principle should be "consistent with the protection of information that needs to remain confidential" and proposed that "certain classes of sensitive information" would have to be exempted from disclosure. The exemptions, the Team proposed, should be narrow, well-justified, designed to prevent real harm and, where necessary, subject to a public interest override. In its initial conceptualisation, the Task Team proposed exemptions to the disclosure requirement if the release of information could cause serious harm to national defence or security; or undermine law enforcement; or jeopardise personal privacy; or jeopardise the government's management of the national economy or the national finances; or jeopardize the safety of an individual; or seriously jeopardize the government's capacity to collect information in the national interest; or jeopardise proper personnel administration in the public service; or jeopardise the deliberative process within the government, by inhibiting candid internal communication (Open Democracy Task Team, 1995).

Their proposal also included the requirement that proactive measures be taken by public bodies to foster a culture of transparency, and that they be routinely required to publish or make available the following kinds of information: manuals or brochures detailing descriptions of the classes of information in their possession, information about their internal structures, functions, responsibilities and decision making processes, the means by which citizens could participate in the bodies' decision-making processes; details of complaint,

appeal and redress procedures available in and over the body; details of public services available from the body and how to use them; and details of internal complaints procedures available to an official who wishes to draw attention to lawbreaking, corruption or maladministration in the body (Interview with Empie van Schoor, 25 August 2003).

The Task Team proposed a number of enforcement mechanisms, including the appointment of an Information Officer by each government body to consider requests for information held by that body. There would be a system of internal appeal to the head of the body, should a request be refused. If such an internal appeal was not successful, a requester would have recourse to an Information Court, which would deal exclusively with the enforcement of the Open Democracy Act. Powers of intervention and mediation would be given to the Public Protector and Human Rights Commission. The Task Team also proposed the establishment of an independent body, the Open Democracy Commission, to monitor the effectiveness of the Act and to report annually to Parliament on its implementation through the appropriate Parliamentary Committee (Open Democracy Task Team, 1995).

The drafting of the Open Democracy Bill did not proceed without its fair share of delays. Between 1995 and 1996, it was submitted to Cabinet twice but referred back for further work and consultation. The draft Bill was published in the Government Gazette in October 1997, for public comment. Comments were considered and further adjustment made, and in 1998, the draft was approved by Cabinet. In 1998 the draft Bill was finally tabled in Parliament. It was proposed that the purpose of the Open Democracy Act would be to give citizens access to information held by public bodies, and access to the proceedings of certain public bodies. Another proposed aim of the Act was to protect privacy. Further, it would provide for the protection of officials who disclosed serious maladministration or corruption. And generally, the Act would empower the citizenry to participate in governmental decision making that affected hem (Currie & Klaaren, 2002).

Originally, it was recommended that the Act should do the work which was sometimes done, in other countries, by separate freedom of information acts (also known as access to information acts), privacy Acts, open meetings acts (also known as "government in the sunshine" acts) and whistleblower protection acts. However, a decision was taken by Cabinet to table a separate bill dealing with the issue of whistleblowers and that of open meetings.

Over time, the open meetings component was abandoned by Cabinet. The legislation providing for the handling of whistleblowers was to be the Protected Disclosures Act, 2000. The reason for the separation had a constitutional basis. Technically, the Constitution required the enactment of access to information legislation before 4 February 2000 (Interview with Empie van Schoor, 25 August 2003).

When it was finally passed by Parliament in 2000, the aim of the Promotion of Access to Information Act was crafted as follows:

> To give effect to the constitutional right of access to any information held by the state; to make available to the public, information about the functions of governmental bodies; to provide persons with access to their personal information held by private bodies; to provide for the correction of personal information held by governmental or private bodies and to regulate the use and disclosure of that information; to provide for the protection of persons disclosing evidence of contraventions of the law, serious maladministration or corruption in governmental bodies; and to provide for matters connected therewith
>
> (Promotion of Access to Information Act, 2000, Aim).

The Act stands among similar models in the world giving effect to transparency and accountability in government, and also on the part of private bodies. It has brought South Africa along way away from the days when much of officialdom was shrouded in secrecy.

Outline of the Act

The Act is a comprehensive document addressing, inter alia, the requirement of all public and private bodies making information about themselves known to the public, how requesters can apply for access to records, the grounds for refusal of access to records, and appeal mechanisms. In the next section I will attempt to summarise the provisions of the Act, highlighting those that are especially relevant in the context of balancing the relationships between secrecy good governance and security in post-apartheid South Africa.

Scope of application of the Act

The Act overrides the provisions of any legislation that might be materially inconsistent or in conflict with its provisions. This means that intelligence services have no automatic recourse to claims of a right to secrecy, and must find the means to balance their objectives (also defined in law), in the provisions of this Act. As shown later, the Chapter on Grounds for Refusal of Access to Records is intended to validate legitimate and justifiable non-disclosure.

Not all public bodies are subject to the PAIA. Significantly, section 12 stipulates that the Act does not apply to a record of the Cabinet and its committees, the courts of the constitutional judicial system, special tribunals established in terms of the Special Investigating Units and Special Tribunals Act, 1996 and officers of such courts or tribunals. Nor does the Act apply to individual members of parliament or provincial legislatures acting in that capacity. The Act however does not preclude Cabinet and its committees, members of Parliament or the provincial legislators from requesting information in relation to private bodies.

The Act qualifies the manner in which information held by the state should be made public, as to be conducted "as swiftly, inexpensively, and effortlessly as reasonably possible without jeopardising good governance, privacy and commercial confidentiality (Section 9b, Promotion of Access to Information Act, 2000).

Moreover, the intent behind such legislation was generally, to promote transparency and accountability of all organs of state by providing the public with timely, accessible and accurate information and by empowering the public to effectively scrutinise, and participate in, governmental decision-making that affects them. (Currie & Klaaren, 2002).

These are important provisions, since they outline a paradigm hich the security and intelligence agencies must take into account, in decisions affecting their implementation of the Act. Members of the public might choose to raise a host of issues for disclosure by the intelligence agencies. These in turn generate the need for appropriate and publicly acceptable policy choices.

It should be noted that the Act mainly provides for access on request and in particular for access to already existing records. A body, to which a request is made, therefore, cannot legitimately be expected to compile a record if it does not already exist. Reading between the lines, the temptation for services to avoid committing matters to recorded form, may well be one of the hazards that theoretically face those who would wish to access information from the intelligence services (Interview with Tertius Geldenhuys, 7 October 2003).

The Act is strongly weighted in favour of requesters. The 1996 Constitution does not require a requester to prove that the information is necessary for the exercise of his or her constitutional rights. The reason for the request is in fact irrelevant, and the onus is on the public or private body to which the request is directed, to comply with any legitimate request. Interestingly, there is a dispute about whether a requester can rely on the Constitution to give effect to the right of access, or must rely on the Act (Currie & Klaaren, 2002).

Routine disclosures required to be contained in the PAIA manuals

Chapter 2 in Part 2 of the Act outlines the information which all public bodies must publish, in a manual, about themselves, in at least two official languages. (Part 3 of the Act has identical requirements for private bodies). The manual must contain a description of the public body's structures and functions, and its contact details. It must list the subjects on which the body holds records, and the categories of records held on each subject. It also has to contain a description of every personal information bank held by the public body. The manual must clearly state which categories of records are open to the public, how to obtain access to those records; in addition it must provide a description of the services available to members of the public from the body, and how to gain access to these services.

Other information that the manual must contain includes a description of the duty of the head of the body to disclose in terms of section 8, records revealing a serious public safety and environmental risk; arrangements for members of the public to participate in or influence the formulation of policy, or the exercise or performance of duties; and remedies available in respect of an act or failure to act by the body. In particular, the manual is required to specify all remedies to a member of the public, or an official who wishes to report or otherwise

remedy an impropriety, and provide for protection for an official of the body against reprisals (Currie & Klaaren, 2002).

Chapter 2 is significant since it is the window through which members of the public gain insight into the role, structure and functions of the public body. In the case of intelligence services, it is probably more significant than in the case of other public bodies, about which members of the public are likely to have some insight through media reports and information that is generally available. The blanket of secrecy around the intelligence services tends to be perpetuated by a routine classification of almost all information about these structures and the absence of a framework for the non-classification or declassification of such information (Interview with Tertius Geldenhuys, 7 October 2003).

Requests for access to information

Part 2, Chapter 3 (Manner of Access) addresses the designation of the Deputy Information Officer, who has direct responsibility for implementing procedures for the processing of requests, as well as the transfer of requests where a public body does not have the required information. It also requires agencies to ensure the preservation of requests until a final decision has been made on granted access. Only the Information Officer or Deputy Information Officer is empowered to respond to a request for access, and not any official of a public body.

Grounds for refusal of access to records

The PAIA recognises that there are circumstances under which public bodies should have the right to refuse requests for information. These circumstances are contained in a chapter dealing with grounds for refusal of access. Technically, according to the Act, refusal is deemed to have taken place if body responds that it cannot find a requested record, or that it does not exist. Refusal is also deemed if a response to the request is not lodged within the regulated time. In case of a refusal, an appeal can thereafter be lodged, first to the body, and then to the Minister.

When a request has been lodged, access to a record may be legitimately refused on a number of grounds clearly stipulated in the Act. The grounds must be justifiable in terms of the Constitution, and both mandatory and discretionary grounds for refusal exist within the law. Another significant feature of the Act is that an Information Officer may deny the existence or non-existence of a record, if it the opinion of the public body that acknowledgment thereof is going to cause harm (Part 2, Chapter 4 Promotion of Access to Information Act).

In summary, a request for access to a record may be refused if the refusal is based on the mandatory protection of the privacy of a third party who is a natural person, or the mandatory protection of tax and certain other records of the South African Revenue Services. Access must also be refused if the refusal is based on the mandatory protection of commercial information of a third party, the mandatory protection of certain confidential information or the mandatory protection of the safety of individuals and of property, where the refusal is based on the mandatory protection of police dockets, or the mandatory protection of research information.

There are also a number of grounds for refusal of access, which are discretionary. In other words, the public body to which the request is directed must weigh whether several duties or responsibilities it has will be compromised. Thus a request for access to a record may be refused if the refusal is based on the protection of certain other confidential information of a third party; if it is based on the protection of law enforcement and legal proceedings; or if it is based on the protection of defence, security, and international relations of the Republic. Refusal may also be effected where a request is manifestly frivolous or vexatious, or where access to a record or records will result in a substantial or unreasonable diversion of resources. However, the Act provides for mandatory disclosure if disclosure is in the public interest, or would reveal substantial environmental risk/harm to public safety (Currie & Klaaren, 2002).

Implications of the grounds for refusal for the intelligence services

There has not been such extensive of review of requests for access to information requests before the South African courts. It would appear though, that the implications of the grounds for refusal are considerable, though weighted in favour of the intelligence services' claim to a

duty of secrecy. My interpretation of the implications of these grounds for refusal, is as follows.

There is a mandatory protection of the privacy of a third party who is a natural person.

This provision in the Act (section 34) is meant to provide for the right of privacy, also enshrined in the Constitution. The implication of this "exception clause" is that a public body cannot make personal information available about a natural person who is a third party, including a deceased individual, to a requester. However access may be granted in some cases, e.g. if the person about whom the information is requested has consented to disclosure; or if he or she has provided the information to the public body, knowing that it might be made available at some stage. Access may also be granted if the information is already publicly available; or if the information is about the physical or mental health of a third party who is a minor under the care of the requester. Finally, access may be granted to a requester if the information is about an individual who is or was an official of a public body, and the information relates to the position of that individual in relation to his or her office.

This exclusion applies most obviously to personal files of individuals held by the intelligence services. This much was implied by Dr Graham Dominy, who in an interview with SAFM in November 2003, confirmed that persons whom apartheid era security services had kept files on, could request to see their own files in terms of the Promotion of Access to Information Act, if the records were more than twenty years old, as prescribed in the National Archives Act, 1996. Access requests would be evaluated, however, and not disclosed automatically. Moreover, a member of the public was not entitled to see another person's file unless such access was in principle agreed to by the person concerned, and after which the request would be evaluated if the files contained no information that was protected in terms of the PAIA, it could be released to the requester. Dominy stressed that a person seeking access to his or her personal file that had been maintained by the security forces, would have to comply with the requirement of the PAIA, completing the necessary forms, and paying the prescribed administrative fees for the processing of the request (SAFM interview with Graham Dominy, November 2003).

Another area in which this exclusion has relevance is that of security screening of members of the public. In taking on new employees, intelligence services routinely acquire information about them (as well as other unsuccessful candidates) through detailed screening processes. In addition, they are sometimes required to investigate and issue security clearances to civil servants occupying positions where access to sensitive information is routine or frequent. Generally speaking, where candidates fail to obtain security clearances, reasons are not supplied. This may have to change, or at the very least, the intelligence services would have to be very thorough in documenting such reasons, in the event of a challenge by an individual requesting access to the records on which such a decision is based.

This provision of the PAIA also has implications for the protection of information about such candidates, and implies a requirement that the intelligence services protect their privacy. It provides the broad guideline that providing personal information to a third party, without the consent of an individual, would be illegal. This indeed is in line with draft concepts on privacy legislation that the South African Law Commission is busy with (Interview with Tertius Geldenhuys, 24 August 2003)

Another implication of this clause is that the intelligence services are not at liberty to make personal information about persons in their ranks available to requesters, without the consent of the individual concerned. This supports the trend or requirement of protecting the identities of intelligence workers and their sources, already provided for in the Intelligence Services Act, 2002.

<u>There is a mandatory protection from disclosure of certain records of the South African Revenue Services.</u>

According to section 35 of the Act, the SA Revenue Services must refuse a request for access to a record if the record contains information obtained or held for the purpose of enforcing legislation concerning the collection of tax revenues. On the face of it, this ground for refusal does not have direct consequences for the intelligence services. However, it begs further consideration. The SARS is reliant for its effectiveness on being able to match bona fide individual identities with income. Intelligence agencies often operate through persons or entities who assume false identities, or details for purposes of operational security.

Mechanisms for ensuring that the earning of these entities are accounted for will have to be put in place. These procedures will need to be transparent enough to withstand the corruption factor - funds generated through front companies finding themselves into the pockets of individuals and not back into state coffers.

There is a mandatory protection of commercial information of a third party.

According to section 36 of the Act, a request for access must be refused by a public body if the requested record contains:

- trade secrets of a third party;
- financial, commercial, scientific or technical information, disclosure of which would be likely to cause harm to the commercial or financial interests of that third party;
- information supplied in confidence by a third party, the disclosure of which might harm their interests in contractual or other negotiations or in commercial competition.

However, access to records may not be refused if the record requested is already publicly available, or if the third party in question has consented to making the information available, or in the case of information relating to product or environmental testing, and its disclosure would reveal a serious public safety or environmental risk. This clause is relevant to the intelligence services insofar as these bodies like other public bodies routinely enter into contractual arrangements with commercial entities. In fact, it may strengthen the preferred arrangement of confidentiality that intelligence services may seek. In some cases, commercial entities are required to keep confidential that they are engaged in a relationship with the services, and very often are themselves required to undergo security clearances and due diligence probes before their involvement with the intelligence service are confirmed.

There is a mandatory protection of certain confidential information, and protection of certain other confidential information of a third party.

Section 37 stipulates that a public body must refuse a request for access to a record if, in disclosing the record, it would breach a duty of confidence owed to a third party in terms of an agreement; or it may refuse access to a record if the record consists of information that was

supplied in confidence, and if its disclosure could possibly jeopardise the future supply of similar information or information from the same source, and if it is in the public interest that such an outcome should be averted.

This provision is clearly of significance to the intelligence services which procure most of the information they hold from confidential sources or informants. In most cases, sources undertake to supply sensitive information on condition that their identities will not be disclosed.

There is a mandatory protection of the safety of individuals, and protection of properties.

In terms of this section 38, a public body must refuse access to a record if its disclosure could reasonably be expected to endanger the life or physical safety of an individual or if the disclosure could prejudice the security of a building, structure or communications system, transport, property, an individual under a witness protection scheme, or the safety and security of the public or property.

This exclusion correlates strongly with the provisions of the Protection of Information Act, 1982, which seeks to prevent and to penalise disclosure of information in relation to the above-mentioned areas.

There is a mandatory protection of police dockets in bail proceedings, and a protection of law enforcement of law enforcement and legal proceedings.

According to section 39 of the Act, a public body must refuse a request for access to a record if access is prohibited in terms of the Criminal Procedure Act, 1977 (Act No 51 of 1977). Alternatively it may select to refuse a record under certain other conditions e.g. where the record contains information about investigative methods and techniques, the disclosure of which may prejudice the effectiveness of the investigation, or may reveal or provide leads as to the identity of a confidential source of information.

This too is a clause of much relevance and support to the agencies of the criminal justice and intelligence sectors. A case can be made for withholding information in the interests of a

successful outcome to an investigative process. Significantly, however, the Act is sensitive to other basic freedoms; in this same clause, it is stipulated that a requested record may not be refused where it consists of information about the general conditions of detention of a person in custody.

In this clause, provision is made for a public body, through its information officer, to refuse to confirm or deny the existence or non-existence of a record; if harm is likely to be caused by such disclosure. Whilst this may appear severe, the Act does carefully stipulate what elements a satisfactory response to a requester should at least contain; moreover, the requester does have the option of lodging an internal appeal.

There is a mandatory protection of records privileged from production in legal proceedings.

Section 41 states that public body must refuse access to a record if the record is privileged from production in legal proceedings, unless the person entitled to the privilege has waived it. This is a general legal principle, to protect the integrity of legal proceedings, which the intelligence services will be a beneficiary of, should its records require protection.

There is a discretionary protection of information related to the defence, security and international relations of the Republic.

According to section 41, public body may refuse access to a record if its disclosure could prejudice the defence, security or international relations of the Republic; or if it would reveal information supplied in confidence by or on behalf of another state or international organisation; or if the information is required to be held in confidence by an international agreement or customary international law.

The above would include information relating to military tactics or strategy or military exercises or operations undertaken in preparation of hostilities, or in pursuit of the detection of prevention of hostilities; information relating to weapons procurement, capacity and development; information relating to force deployment and characteristics; and information held for intelligence purposes.

Here again, the Act appears to be aligned in its intention, with the provisions of the Protection of Information Act, 1982. In fact, through these and other provisions, it is quite generous in ensuring that the intelligence and security services are not disabled. The provisions are sufficiently broad to refuse disclosure, and give the information officer of the public body discretion in disclosing information or not. Also, the information officer may refuse to confirm or deny the existence or non-existence of a record, if it is thought that to refuse or deny would in either case prove harmful to the interests of the state.

There is a discretionary protection of information relating to the economic interests and financial welfare of the Republic, and the commercial activities of public bodies.

According to section 42 of the PAIA, access may be refused where information held by a public body is likely to jeopardise the economic interests or financial welfare of the republic, or the ability of the government to manage the economy of the Republic in the best interests of the Republic. This could include information on contemplated changes in policies affecting currency, coinage, legal tender, exchange rates or foreign investment; the government's position in relation to credit or interest rates, customs or excise duties taxes or other revenues; the regulation or supervision of financial institutions; government borrowing and international trade agreements.

There is a mandatory protection of research information of a third party, and protection of research information of a public body.

Where a third party could be exposed to serious disadvantage, a record which contains information about research being conducted by or on behalf of the third party may be withheld (Promotion of Access to Information Act, 2000, section 43). This presumably is also a provision which could be utilised by the intelligence services, which is client -driven in its provision of intelligence reports. It could be argued that a client, such as the President of the Republic or the Cabinet, could be disadvantaged if the studies it is commissioned to undertake, are made publicly available.

There is a discretionary protection of the operations of public bodies.

In terms of section 44 of the PAIA, information can be withheld from public disclosure if the record sought contains information relating to an opinion, advice, report or recommendations obtained or prepared, or flowing from a consultation, discussion or deliberation, for the purpose of assisting to formulate a policy or take a decision in the exercise of a power or performance of duty, and if disclosure could inhibit further candid communications and deliberations within the public body (Section 44, Promotion of Access to Information Act, 2000).

In essence, this provision serves to shield the public bodies from scrutiny pertaining to their inner workings. It could be readily utilised by intelligence agencies to ensure that sensitive minutes or policy documents are not made publicly available.

There is a discretionary protection from manifestly vexatious or frivolous requests.

Section 45 states that where a request is manifestly vexatious or frivolous, and the work involved in processing the request would amount to a substantial diversion of resources, a request for access may be refused. This is an interesting exception, and any public body refusing a request on these grounds would have to consider carefully in what way a request could be described as frivolous, as a requester would probably argue that gaining the information is important to them. In any event, the PAIA does not require a requester to justify wanting access to a record; it is simply an incontestable right if the information requested is requested for the exercise or protection of the requester's rights and if the information or record thus requested is not covered by the grounds for refusal.

There is a mandatory requirement of disclosure if it is in the public interest.

Lastly, section 46 of the Act provides for mandatory disclosure where this would reveal evidence of a substantial contravention of or failure to comply with the law, or an imminent and serious public safety or environmental risk, of a nature so grave that the public interest in the disclosure outweighs the harm contemplated.

Appeals

Part 4 of the Act covers appeals against decisions. Within stipulated time frames, a requester may launch an internal appeal with a public or private body which refuses access to information. If the internal appeal procedure has been exhausted and the requester is still unsuccessful, the requester may apply to a court for relief. The courts are empowered to hear representations in camera; and may prohibit the publication of proceedings where so appropriate. The burden is on the refusing body to demonstrate the veracity of its stand. These conditions – of the confidentiality of the presentation of argument - work to the favour of the intelligence services.

Functions of the Human Rights Commission

Part 5 of the Act addresses the functions of the Human Rights Commission (HRC) in relation to the Act. The HRC is charged with the responsibility of popularising the Act, and monitoring its implementation. It also has to train information officers of public bodies, and provide advice on how to administer the Act. The HRC must make recommendations on the development, improvement, modernisation, reform or amendment of the Act or other legislation or common law having a bearing on access to information held by private or public bodies. And it has to annually provide detailed reports to the National Assembly, on how each public body has fared in relation to the implementation of the Act.

Other aspects covered in the Act

Part 6 covers Transitional Provisions in at least two significant respects. Firstly, the Minister has to make further legislative provision to ensure that Schedules 1 and 2 of the Act are completed. And it makes provision for extended periods for dealing with requests during the first two years.

General provisions are covered in Part 7, the last part of the Act. It stipulates a person who attempts to deny a right of access to a record through its willful destruction, damage, alteration, concealment or falsification is liable for up to two years' imprisonment. And it requires the Minister to provide regulations for the implementation of the Act. Such

regulations must be submitted to Parliament before publication. Provisions of the Act may be brought into operation on different dates.

Implications of the overall legal framework for secrecy and transparency

The post-apartheid intelligence services find themselves in dilemmas similar to those with which security and intelligence services in democracies around the world must contend. The very existence of an intelligence capacity within the South African state machinery, presupposes the existence of threats or potential threats to that state. Such a capability is usually afforded the licence to conduct its work - of detecting and forewarning government about such threats - in conditions of relative secrecy. Potential conflicts arise when possible infringements on the public's right of access to information are introduced. And where the legal framework enforces other rights, such as the right to privacy, the intelligence services must strive to strike the right balance here as well. This is especially the case where citizens may be the object of their intelligence gathering operations, e.g. in the case of security clearance investigations, or when the intelligence service investigating an individual's role in activities perceived to threaten national security.

Whilst there has been a fundamental constitutional change, there has been to some extent continuity between the apartheid and post-apartheid era security framework, particularly insofar as the conditions regulating secrecy are concerned. Access to information, in this context is a new challenge, guaranteed as a right only since the end of apartheid. Thus, the legal framework within which the intelligence services function, makes provision for access to information, but at the same time authorises sweeping measures for the "protection" of information. The grounds for refusal in the PAIA make ample provision for the intelligence services to withhold information from disclosure. In addition, the post-apartheid regulatory framework provides additional leverage for the cause of transparency: there exists today, a range of institutional mechanisms that determine the space in which intelligence services function, including the legislation around intelligence which provides for a multi-party oversight committee and an Inspector-General, the Public Finance Management Act, and the Auditor-General Act, among others.

The Protection of Information Act, 1982 has been amended to extend the definition of a security matter to include information generated by the post-apartheid intelligence services. The Act has the legal force that the MISS lacks, and is therefore prosecutable. Critics however, have argued that it is unnecessary to retain it, since the constitution proceeds from the basis of a right of access to information, and provision is made for the protection of information related to the defence, security and international relations of the country.

The problem with the above analysis is that the PAIA is intended to promote access to information. A case can be made to elaborate, using the PAIA grounds for refusal, legislation that gives effect to the duty of the state to effect the protection of information. Such legislation could spell out the procedures for protecting information, penalties for non-compliance, and other aspects that are not spelt out in the PAIA. We therefore examine in the next section of this chapter, how other countries have attempted to address these issue.

Comparative international experience

In the decade following the end of the Cold War, large number of countries adopted freedom of information legislation. They included Japan (1999), South Africa (2000), South Korea (1996), Iceland (1996), Thailand (1997), the United Kingdom and a number of East and Central European countries, which join countries which enacted such laws a considerable period ago including Sweden (1949), the USA (1966), the Netherlands (1980), Canada (1982) and Australia (1982). This phenomenon - of adopting freedom of information legislative regimens - reflects the demands of the countries' respective populaces for greater accountability on the part of their governments and other public bodies, especially following crises of confidence – usually around the management of security matters or foreign relations. Given that security and intelligence organizations operate largely in secret, a study of how the access to information legislation has impacted on the functioning of such entities in democracies is warranted, and may be instructive in the South Africans arena. It has to be remembered however, that various access to information systems are borne out of differing historical circumstances, in relation to differing concerns to various parliamentary democracies. Notwithstanding this, it is helpful to take note of the experience of various countries and to understand the contradictions that often have to be grappled with when

weighing the interests of national security and the public's right of access to information. South Africa may benefit from taking these experiences into account, and may even be in a position to anticipate and prepare policy positions for certain categories of requests.

United States of America (USA)

Being a country with a long-established freedom of information dispensation, the United States is often looked at for the answers to the issues surrounding this matter. Yet it is important to remember that in the USA, freedom of information arose out of particular historical conditions.

Origins of the USA Freedom of Information Act

The Freedom of Information Act (FOIA) was enacted by Congress in 1966, and introduced a general right of access to public records. This was felt necessary because of the increasing resort by state departments to secrecy, often cited as justified in view of Cold War imperatives. Whilst the various states, to differing degrees had chosen to introduce various forms of open government, prior to 1966 there existed no general right to inspect federal records. A provision of the Administrative Procedure Act had made federal records available to "persons properly and directly concerned" subject to vague exceptions intended to protect the public interest and without any supporting judicial remedy. Since this provision in effect became a charter to withhold rather than an instrument of disclosure, it was ultimately repealed and replaced by the FOIA (Adler, 1991).

The FOIA is better understood in the context of other laws impacting on access to information, and balancing the interests of the individual. One such law is the Government in the Sunshine Act ("Sunshine Act") passed in 1976, and founded on the view that the government should conduct the public's business in public. This Act applies to all agencies which are subject to the FOIA, and opens the meetings of these agencies to the public.

The Sunshine Act contains exemptions which mirror closely those found in the FOIA. Another development has been the adoption of the Privacy Act of 1974, which reinforces the

constitutionally protected right of privacy of American citizens. Congress in acknowledging that this right is affected by the collection, use and dissemination of personal information by the federal agencies, heightened by the use of computers and technology, has south to regulate these practices through this Act. This includes a system of access by individuals to records about themselves, with exception.

Main features of the USA Freedom of Information Act

The basic idea of the FOIA is that all records of agencies of the federal government must be accessible to the public, unless exempted from this requirement. Any member of the public ("any person") may request a record – the Act does not stipulate a citizenship requirement, and the courts' interpretation is that the definition includes foreign citizens, corporations and governments. Generally speaking, a requester is under no obligation to submit a reason for the request for example to prove t information is necessary for the exercise of his or her rights. In addition, the Act provides for response times to requests, costs of making requests and an appeals mechanism.

In the beginning, there was resistance on the part of some agencies who employed a variety of means to discourage the use of the Act, including high fees, long delays and claims that they could not find the requested materials (Adler, 1991).This led to a review of the Act and the introductions of various amendments in 1974. Minor amendments were effected in 1976, dealing with standards to determine more precisely which "other statutes" could be used as grounds for withholding information, and in 1986, amendments concerning fees policies, and access to certain law enforcement and national security records were enacted.

Over time, there was concern by the US government that confidential sources, ongoing investigations, and certain manuals and other sensitive non-investigative law enforcement materials were not adequately protected from disclosure by the Act's exemptions. Thus the following exclusions came into force with the 1986 amendments: records whose disclosure would interfere with criminal proceedings of which the subject is not aware; informant records requested by a third party according to the name or personal identification by which it is maintained; and classified records of the FBI pertaining to foreign intelligence, counterintelligence or international terrorism.

Grounds for refusal (exemptions)

In its current form the following exemptions are provided for in the FOIA: national Security information, internal agency rules; information exempted by other statutes; business information; reverse FOIA litigation; personal privacy; law enforcement records; the records of financial institutions, and oil well data.

Of particular relevance to intelligence is Exemption 1, which states that the FOIA does not apply to matters that are specifically authorised under criteria established by an Executive Order to be kept secret in the interest of national defence or foreign policy and are in fact properly classified pursuant to such an Executive order. It should be noted however, that the security and intelligence services of the USA are not excluded from the provisions of the Act; indeed they have been the target of civil rights groups and a massive body of case law has developed around the courts' application of the Act.

The USA makes statutory provision for the protection of classified information. It also clarifies by Executive Order (No. 12356), which has the force of law, what information shall be classified. These categories are military plans, weapons or operations; the vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security; foreign government information; intelligence activities (including special activities), or intelligence sources or methods; foreign relations or foreign activities of the United States; scientific, technological or economic matters relating to the national security; United States Government programs for safeguarding nuclear materials or facilities; cryptology; a confidential source; or other categories of information that are related to the national security and that require protection against unauthorized disclosure as determined by the President or by agency heads or other officials who have been granted original classification authority by the President (Adler, 1991).

Status of Central Intelligence Agency (CIA) operational files

As stated earlier the USA's security and intelligence agencies are not as a class, exempted from the provisions of the FOIA. Adler (1991) informs us however, that in 1984, Congress

amended the National Security Act of 1947 to authorize the Director of Central Intelligence to exempt certain "operational files" of the Central Intelligence agency (CIA) from the search and review requirements of the FOIA. Significantly, this amendment was passed with the support of the American Civil Liberties Union, a vocal freedom of information advocacy organization. Through this statute, Congress hoped to relieve the agency of its frustrating administrative burden in having to search and review certain files that 'almost invariably prove not to be releasable under the FOIA' thereby reducing the processing backlog and delays in responding to FOIA requests, 'while preserving undiminished the amount of meaningful information releasable to the public,' and providing additional assurance of confidentiality to CIA sources (Adler, 1991).

The definition of operational files included files of the Directorate of Operations which document the conduct of foreign intelligence or counterintelligence operations or intelligence or security or liaison arrangements or information exchanges with foreign governments or their intelligence or security services; files of the Directorate for Science and Technology which document the means by which foreign intelligence or counterintelligence is collected through scientific and technical systems; and files of the Office of Security which document investigations conducted to determine the suitability of potential foreign intelligence or counterintelligence sources. Significantly, files which are the sole repository of disseminated intelligence, are not regarded as operational files (Adler, 1991).

Impact of freedom of information legislation in the USA

Freedom of information has been used extensively in the USA to defend and uphold constitutional rights. Co-existing in a political environment which has simultaneously given attention to the challenges of classification and declassification, access to information has always been an issue around which the intelligence agencies could not afford to be complacent. The consequence has been that there is a culture of public information about the workings of the intelligence community, translating into the many courses offered by universities, academic research, and a critical media.

In the USA, The Commission on Protecting and Reducing Government Secrecy (Moynihan Commission, 1997) observed that there had always been a great deal of subjectivity on the

part of officials in their interpretation of classification and declassification criteria, and consequently much inconsistency in the application thereof. Because there was no statutory basis for this secrecy system, each time there was a change of administration, a new Executive Order on classification and declassification was issued. The report of the Commission remarks on the disruptive effect of these regular amendments on the efficient administration of the classification system. Quite often, dissenting public officials simply dragged their feet on implementing policy changes, with the understanding that with the appointment of the next administration there would be yet another change.

The Moynihan Report also expressed concern over the reliance on the Freedom of Information Act as an instrument for declassification. The limitation of the FOIA is that it is only effected when individual requests are made; Naturally, it is difficult for interested parties to make requests about secrets. The agencies of whom such requests are made are at an advantage in that they can sever substantial chunks of information which might have provided the requester with significant contextual information if the declassification process was more inclusive Concern is therefore expressed by the Commission that a culture of openness will never develop unless the culture of secrecy is restrained The Commission therefore recommended mechanisms for the proactive declassification of intelligence records and oversight structures to ensure compliance with this process (Moynihan Commission, 1997).

The USA intelligence services are subjected to extensive and public scrutiny, making for a significant degree of transparency about the intelligence services. Congressional committees, several government initiated reviews, a culture of litigation, the presence of civil liberties organisations, have all contributed to a significant amount of information and records about the services being placed in the public domain, over the years.

Canada

Freedom of information is dealt with in Canada less than two pieces of legislation: the Access to Information Act of 1982 and the Privacy Act, 1982, which are seen as complementary and balancing features.

Origins of Canada's Access to Information Act, 1982

The legislation came into being at a time when Canada was undergoing substantial constitutional reform, introduced by the Trudeau government. At the same time there was growing controversy over the role of the security forces – in particular the Royal Canadian Mounted Police. The result of the McDonald Commission, set up to investigate abuses by the RCMP, was the establishment of a civilian intelligence agency, the Canadian Security Intelligence Service (CSIS), in 1984.

The Canadian legislation covers all federal agencies including the security services. In addition several regional authorities, including Ontario, Quebec, British Columbia and Quebec have also introduced access to information legislation, covering thousands of institutions, as opposed to 132 covered by the federal legislation.

Main features of the Act

The Access to Information Act, 1982 promotes the following principles: government information must be made available to the public; exceptions to the right of access should be limited and specific; and decisions on disclosure should be reviewed independently of government. In Canada, use of the Access to Information Act is restricted to citizens and permanent residents or persons present in Canada, thereby excluding foreigners. The security and intelligence agencies are not excluded from the ambit of the Act.

The Canadian Security Intelligence Service (CSIS) is required to and has complied with this requirement to publish information about their information holdings, and lists the following as included in the range: communications security, planning and coordination of CSIS activities, information about counter-intelligence and counter-terrorism, information on access and disclosure procedures and requests, personnel records, internal security of the Service, scientific, operational and technical support, on the supply of security assessments to other government departments, and on the policy, administration and management of operations involving human sources (Hazell, 1989).

The Act creates an obligation for a public body to disclose a record if there is such a request. The general principles are that there is no obligation on the part of a government body to create a record if it does not exist.

CSIS receives requests from a wide range of sources including historians, many of whom admit to submitting similar requests before several agencies in the hope of getting as comprehensive an answer as possible. This is partly because CSIS makes frequent use of the provision in the Act, to neither confirm nor deny the existence of information on current operations; the main concern seems to be to able to provide lifelong protection for those who have acted as human sources.

As in most of the country examples, the following kinds of information are protected from disclosure: national security and defence; international relations; law enforcement;
Cabinet discussions; civil service advice; legal advice; damage to the economy; commercial information; Personal information; and information protected by other statutes.

Canada has a diverse system of controls over the security and intelligence community in place, and thus a fair measure of public accountability in this area of governance. The Mc Donald Commission had recommended and there was established an independent body to review the functioning of the CSIS. The members of the Security Intelligence Review Committee (SIRC) are all privy councillors, appointed by the governor-in-council after consultation by the prime minister with leaders of the major opposition parties. The SIRC performs four major functions: it must review CSIS's performance of its duties; it must investigate the complaints of any persons against the CSIS; it must investigate complaints regarding security clearances, and it must review cases concerning national security matters. SIRC releases an annual report to the public about its work, and generally has inspired public confidence about its role (Rankin, 1986).

Another mechanism of control is the Inspector-General, appointed by the Cabinet. Like the SIRC, the Inspector-General as wide access to documentation of the CSIS, excluding cabinet records. In the Canadian example, the solicitor-general is the minister responsible for the CSIS, the inspector-general and the SIRC. All three report to him/her, giving effect to the principle of ministerial responsibility (Rankin, 1986).

Canada as a country has, like many others, learned the lesson of allowing the security services to function under conditions of unaccountability. The legislative measures put in place to address this situation are impressive, yet not without problems. An observation has been made that the case history is not particularly helpful in developing the application of the act. Notwithstanding this a useful comparative basis exists for South Africa, which as adopted many features not only of the legislation around access, but also that dealing with the functioning of the security service.

India

Even though India is an established democracy, like South Africa, it is beset with problems - a colonial legacy which includes a Westminster system of government and the vestiges of many of the laws which Britain applied in its dominions, an economically stratified society, of deep social, religious and caste divisions and a volatile political climate.

In spite of these problems, India is considered to be the largest parliamentary democracy in the world. Its main neighbours are Pakistan, China, Bangladesh and Nepal. Its conflicts with its neighbours, particularly Pakistan, are well documented. Internally, Indian politics is fraught with conflict, which has sometimes claimed civilian lives in scores. Yet in spite of these conditions, the right to information has been an issue throughout the decades of freedom.

Origins of India's Right to Information Act, 2005

The Indian government has for several decades been under pressure to introduce access to information legislation, eventually materialising in the introduction of a Bill at federal level in 1999. The genesis of the right to information goes back to 1975, when the Supreme Court in the State of Uttar Pradesh versus Raj Narayan case, acknowledged that although the right to information was not written into the Constitution, it was implied in the right to freedom of speech and conscience. The Supreme Court of India later ruled in 1982 - in the SP Gupta versus President of India case - that access to government information was an essential part of the fundamental right to freedom of speech and expression. The Court stated:

> The concept of an open government is the direct emanation from the right to know which seems implicit in the right of free speech and expression guaranteed under Article 19 (1) (a). Therefore, disclosures of information in regard to the functioning of Government must be the rule, and secrecy an exception justified only where the strictest requirements of public interest so demands. The approach of the Court must be to attenuate the area of secrecy as much as possible consistently with the requirement of public interest, bearing in mind all the time that disclosure also serves an important aspect of public interest.
>
> Supreme Court of India, 1982

The Indian government established a working group that drafted a bill in 1997. The draft bill, it was proposed, would provide a general right of access to information, and create a National Council for Freedom of Information and State Councils. In February 1999, President KR Narayan announced that the government planned to bring introduce the Freedom of Information Bill.

The Bill was strongly resisted, particularly by public officials (India Together, 2006). It underwent a chequered introduction and a version that was passed in 2000, was discredited for what was considered to be a half-hearted commitment to freedom of information. The Act was withdrawn after a short existence and replaced by a version that satisfied at least some of the concerns of its critics.

Broader legislative context of the intelligence services

Reference has already been made to India's strained relations with its neighbours. This has forced it into a defensive security posture, in which national security is equated with a strong intelligence and defence capability to protect its territorial integrity in a regional context, and a strong police and domestic security posture to counter perceived domestic threats to security. In a sense there is a significant continuity in the needs served by the security institutions. Under British rule, they served to protect British interests; on attaining

independence they were converted to serve the interests of the ruling elite and found themselves increasingly at odds with marginalized political groups (Subrahmanyam, 2000).

The application of freedom of information legislation must be read against a background of the organization and responsibilities of security and intelligence agencies not being established or regulated by legislative acts of the Parliament of India. Nevertheless a plethora of laws exists regulating public safety and national security and the impact of these on public access make for an instructive study: the Official Secrets Act; Criminal Procedure Code; Indian Telegraph Act; Armed Forces Special Powers Act; Disturbed Areas Act; Public Safety Act; National Security Act; and the Terrorist and Disruptive Activities Act (FAS Intelligence Resource Programme , 2001).

Main provisions of the Freedom of Information Bill

One of the legacies of British rule was the Official Secrets Act, which made it an offence to disclose classified information. The Freedom of Information Bill, once passed by Parliament was to take precedence over the Official Secrets Act of 1923. The Bill was for the use of Indian citizens only. The Bill was to be applicable to all federal public authorities requiring them to maintain records which should be subject to disclosure on request (Article 4). Article 5 and 6 of the Bill required public authorities to appoint Public Information Officers, and assist persons wishing to access information, including reducing oral requests into written form. Article 7, dealing with refusals, does not indicate clearly whether reasons for refusal must be given in writing or orally.

Exclusions and Exemptions

Article 16 of the Bill provided for a blanket exclusion of all intelligence and security organizations listed in the schedule, which the central government may amend by notification. Not surprisingly, the legislation adopted by states is very much aligned to the national Act, with regard to the matter of exclusions. One of the first states to adopt freedom of information legislation was Rajasthan. The Rajasthan Right to Information Act, in Section 5, includes the following categories of information where grounds for refusal of disclosure apply : information whose disclosure would prejudicially affect the sovereignty and integrity

of India, security of the State, conduct of international relations, including information received in confidence from foreign Governments, their agencies or international organizations; information the disclosure of which would prejudicially affect the conduct of Centre-State relations, including information exchanged in confidence between the Central and State government or any of their authorities/agencies; information whose disclosure would harm the frankness and candour of internal discussions, including Cabinet papers, interdepartmental/intradepartmental notes, correspondence and papers containing advice and opinions relating to internal policy analysis.

Regarding the federal legislation, the Bill was finally passed as the Right to Information Act, and became operational on 12 October 2005 (India Together, 2006). The Act is for the use of Indian citizens only. Unless scheduled, the Act is applicable to all federal public authorities requiring them to maintain records which should be subject to disclosure on request. Article 5 and 6 of the Bill required public authorities to appoint Public Information Officers, and assist persons wishing to access information, including reducing oral requests into written form. Provision is also made for an internal appeal to a designated individual or office within the public body to which the original request was made. There is a blanket exclusion of all intelligence and security organizations listed in the schedule to the Act, which the central government may amend by notification (India Together, 2006).

Impact of the Right to Information Act, 2005

In summary, it has to be said that the introduction of freedom of information legislation augured well for India, though the categorical exclusion of the intelligence services from the ambit of the Bill suggests that they will continue to work with the public afforded little official information about their functioning.

Lessons for South Africa from the international examples

There are many lessons that South Africa can derive from studying the access to information systems and legislation of other countries and their relevance to the intelligence services. There is firstly, the matter of the application of such legislation to the intelligence agencies. In

some countries, e.g. India, the security and intelligence agencies are specifically excluded from the ambit of the access to information legislation, whilst in others, the USA and Canada, the intelligence agencies are subject to freedom of information legislation.

Freedom of information regimes implemented by governments have generally been the result of pressure from below, usually after the uncovering of a political scandal, and as such represent an important space of political contestation in which the tendency is for the security agencies to resist the opening thereof.

The difference in origins seems to be of little import because one area in which there is seemingly universal commonality is in the range of exceptions. Generally, the following categories of information are exempted from disclosure: private information about individuals; information relating to defence, security, and international relations; information about investigations in the law enforcement sector, particularly if they are ongoing; commercial information, economic information; and operational procedures of public bodies. In relation to intelligence the scope covers the identities of sources and intelligence officers. Thus, even where the intelligence services are subject to the access legislation, provision is made to protect their information holdings from disclosure.

Official secrets legislation or regulations generally coexist with freedom of information legislation. The introduction of the latter has certainly not spelt the death knell for official secrecy. Indeed it has been largely a given that the state's right of refusal to disclose security and defence information, is inalienable. This makes the need for regimens for managing the classification and declassification of information especially relevant.

Some countries have introduced separate legislation to protect the privacy of the individual. This ensures that persons have access to legislation about themselves, and that such information generally may not be divulged to persons not authorized to access it. However, such legislation also generally excludes "national security" information.

Some countries have a well established body of judicial precedence (e.g. USA) but in others this is not the case (e.g. Canada). Moreover, the lack of application of the legislation to the

security and intelligence services in some countries means that they cannot be uniformly looked at for guidance.

There is a trend in all cases for the access to information legislation to be coupled with other mechanism for promoting oversight. These include parliamentary oversight bodies - in the case of Canada a privy council - and also Inspectors reporting to a minister. In spite of the above similarities, South Africa, whilst standing among a body of countries which has adopted freedom of information legislation, has done so in a specific conjuncture, responding to specific pressures, and is at a particular level of maturity in the evolution thereof. It is therefore necessary to be rather circumspect in deriving lessons from other country examples.

Concluding remarks

In outlining the historical background to the Promotion of Access to Information Act, its constitutional basis was highlighted. All in all, the PAIA had its roots in the very cornerstone of South Africa's democracy, the Constitution. Moreover, the legislation is located in a political environment considerably enriched by other institutions promoting transparency and governmental accountability.

The inclusive scope of the constitutional and legislative provisions regarding access to information is unequivocal; they are intended to apply to all state organs, including the intelligence services, which by their nature must maintain a degree of secrecy about some of their activities. To mitigate the consequences of excessive transparency, the right of access is subject to reasonable and justifiable limitation.

The Promotion of Access to Information Act, 2000 makes provision for a number of exceptions where disclosure may be denied. There is thus a legal obligation on the part of the state organs (public bodies) to comply with its provisions, and no public bodies are excluded. Grounds for exceptions are covered in the legislation, and provision is made to exempt certain categories of official information from public disclosure. On assessment, it appears that there is sufficient room for the protection of sensitive information in the Act. The main aim of the Act however, is to promote a culture of openness, a new operating discourse with which intelligence services have yet to become comfortable.

Given that the post-apartheid Constitution and now national legislation requires all state agencies to reveal records requested unless such revelation is excluded in terms of an exception clause, the intelligence services have no option but to cope with the transparency paradigm of the post-apartheid dispensation. The issues confronting them in their choices around secrecy and transparency, and the implications or consequences of these choices for the identity, functioning and sustenance of these agencies, their relationship with the state at large, and the public's right of access to information, are large**.** Both the experience of secrecy under apartheid, and the international experience appear to have relevance to the choices available to policymakers in balancing secrecy and transparency today.

My hypothesis, as set out in Chapter One, is that there was a degree of continuity in the management of security-related information, straddling the apartheid and post-apartheid eras. In addition there are unique and new conditions requiring solutions relevant to the complexities of the day. New legislation includes the Electronic Communications and Transactions Act of 2002 and the Prohibition of Monitoring and Regulation of Interceptions Act of 2002.

The implications of privacy or data protection legislation must be considered. In several foreign jurisdictions privacy legislation and access to information legislation are viewed as being complementary: it is deemed necessary to balance the public right of access to information, with the right of individuals to protect and remain in control of information about themselves.

CHAPTER SEVEN

APPLICATION OF THE PROMOTION OF ACCESS TO INFORMATION ACT IN THE INTELLIGENCE SERVICES UP UNTIL AUGUST 2005

The aim of this chapter is to discuss the strategies pursued by the intelligence services in balancing the competing requirements of secrecy and transparency, in the light of the passing of the Promotion of Access to Information Act, 2000 (the PAIA). It assesses whether these strategies have made for effective and accountable governance of the intelligence services. It also analyses the policy choices around transparency in intelligence, in view of the Act, expressed through institutional arrangements and through the actions and statements of policymakers in government.

The chapter examines whether guidelines for compliance with the provisions of the PAIA exist in the services, focusing of the production of manuals, processing of requests for access, reporting to the Human Rights Commission and initiating voluntary disclosure. In addition, two case studies, examining the manner in which government departments have responded to requests for intelligence-related information, are also presented. One is the response of the Department of Defence to a request for access to records relating to a tender process in the much-publicised Strategic Arms Procurement Package or "arms deal" initiated by government. The other case study concerns the responses of the National Intelligence Agency and the Department of Justice and Constitutional Development to a request by the SAHA for access to records relating to the Truth and Reconciliation Commission. In both cases, there was reluctance by the public bodies to disclose some of the requested information. The research reviews the criteria and processes applied by various stakeholders in evaluating the merits of the requests, and investigates whether the standards applied by the two departments were similar, different or even contradictory.

Overview of implementation of the Act

The PAIA was assented to by President Thabo Mbeki on 2 February 2000. The Act was originally scheduled to come into effect on 15 September 2000, but its implementation was delayed till March 2001 to enable the drafting and approval of regulations required. The first

draft interim regulations were published on 10 August 2001. PAIA sections 10, 14, 16, 51 came into operation on 15 February 2002. However, capacity for the implementation of the Act was limited and all public bodies and private bodies under section 14(4) and 51(4) were exempted from the submission of the manuals contemplated in terms of terms of the provisions in sections 14 (1) and 51(4) from 15 August 2002 to 28 February 2003 (Interview with David Porogo, 27 August 2003).

In 2003, a further reprieve was granted by the Minister of Justice and Constitutional Development: all public bodies and private bodies under sections 14(4) and 51 (4) were exempted from the submission of the manuals contemplated in sections 14(1) and 51 (1) for the period 1 March 2003 to 31 August 2003. All private bodies, except any company not being a private company as contemplated in the section 20 of the Companies Act 61 of 1972, were exempted from compiling the manual contemplated in PAIA section 51 (1) for a period of two years, from 1 September 2003 to 31 August 2005. The SASS and the NIA were both exempted from the compilation and making available of manuals for the period 2003 to 2008 (Interview with Marlyn Raswiswi, 4 August 2005).

Former Open Democracy Task Team member, advocate Van Schoor was critical of the fact that the regulations for administering the Act were not ready for several years after the Act had been passed and said that to avoid delays, one of the lessons of the whole process was that drafting the legislation and drafting the regulations should begin almost simultaneously (Interview with Empie van Schoor, (25 August 2003)

Deputy Information Officer in the DOJ, David Porogo blamed the delay in implementation on yet other factors. He claimed that implementation, for which the DOJ had overall responsibility, had not been linked to the budgeting process of the department. Practical measures, such as the development and distribution of educational material, were therefore affected (Interview with David Porogo, 27 August 2003).

According to Porogo, there was generally a low level of compliance with the requirement that public bodies produce manuals, as with other provisions that required compliance. He indicated that from his observations, a startling number of heads of department were unaware of the provisions of the Act, including their own roles as Information Officers, or that they

were required to appoint Deputy Information Officers in terms of the Act (Interview with David Porogo, 27 August 2003).

Capacity of the intelligence services for implementation of the PAIA

As at the end of August 2005, NIA and SASS displayed varying degrees of preparedness for the implementation of the PAIA. NIA had a policy regulating its implementation of the Act, titled "Policy on the Procedures on the Disclosure of Information". The Director-General of the NIA, Mr Billy Masetlha said that the policy indicated that the General Manager of the structure responsible for Intelligence coordination would serve as the Agency's primary Deputy Information Officer (DIO) and the General Manager of the structure responsible for Security as the secondary DIO. The DIOs were responsible for ensuring proper administrative measures for compliance with the Act, the compilation of responses to requests for consideration and approval by the Information Officer, and any other duties for compliance with the PAIA delegated to them by the Director-General. The policy, as a whole, however, was classified "Confidential" and was not publicly available to those wanting to understand the procedure NIA applied when considering requests (Interview with Billy Masetlha, 4 August 2005).

SASS, on the other hand, only had a draft policy, also classified "Confidential" at the time, which was yet to be approved by the Director-General. A DIO had not as yet been appointed. The SASS draft policy was concerned more with distinguishing information which required protection from that which did not, and not the procedures to which requests for information would be subject (Interview with Hilton Dennis, 25 July 2005).

This contrasted with the situation in the DOD which had both a policy which outlined roles, responsibilities and mechanisms for the implementation of the PAIA. This policy had been approved by the Plenary Defence Council, the highest policymaking body in the DOD. The DOD has two components to its structure: the Secretariat, falling under the Secretary for Defence, who is also the Accounting Officer for the Department, and the South African National Defence Force, headed by the Chief of the SANDF. The Secretariat and the Defence Force each has its own management and accountability structures, leading up to the Minister of Defence, but on a monthly basis, a Plenary Defence Council brings together the most

senior management of the two components. The Plenary Defence Council is chaired by the Secretary for Defence and the Chief of the National Defence Force in alternating months (Interview with Wayne Hendricks, 28 July 2005).

According to Hendricks, a former DOD official, the policy regulating implementation of the PAIA in the DOD was approved in 2000. The Policy was classified "Restricted", and its handling instructions indicated that "this document is the property of the Department of Defence and shall be issued only to those members requiring it in the execution of their duties" (Department of Defence, 2000).

The policy was an update of an earlier policy document, which had been promulgated by the DOD in 1999, in response to the introduction of the Open Democracy Bill in Parliament. As Accounting Officer, the Secretary for Defence was designated as Information Officer (IO). DIOs were to be the heads of the various structures in both the SANDF and the Secretariat. The policy, in line with the provisions of the PAIA spelt out the roles of the IO, as the following: to appoint, direct and control the DIOs; to render or make available such reasonable assistance as necessary to enable a requester to comply with the prescriptions regarding requests for information; to grant or refuse access to information in the possession of or under the control of the DOD; to receive internal appeals against decisions of the DOD; to forward such appeals and reasons for decisions to the Minister of Defence; to assist the Minister of Defence in further dealing with appeals; and to ensure compliance with the Act in the DOD (DOD, Policy on the implementation of the Promotion of Access to Information Act, 2000).

The responsibilities of the DIOs were also spelt out, and included the following: to develop internal procedures to implement the Act in their areas of responsibility; to ensure that persons to whom responsibilities were delegated, were trained in such procedures and stipulations of the Act; and to make recommendations regarding the release of information under their control. The DIO was also required to refer disputed or contentious recommendations to the Information Act Advisory Committee for consideration, to liaise with requesters on all matters pertaining to requests, and to assist the IO and the Minister of Defence in dealing with appeals (DOD Policy on the Implementation of the Promotion of Access to Information Act, 2000).

The DOD policy made provision for an Information Act Advisory Committee, to advise the IO on recommendations from the DIOs, regarding requests for information. The IAAC was to consist of a representative of the IO (chairing the Committee), a representative of the Chief of the SANDF, a representative from Directorate Legal Support, a representative of Defence Intelligence, and the head of the Information Centre.

According to Hendricks, the Justice College under the Department of Justice and Constitutional Development (DOJ) had given training to DOD representatives from different divisions. The week–long training, which had been available to all government departments, was significant because it emphasised the constitutional basis of the PAIA, and the fact that apart from those cases where exemptions were provided for in the Act, there was a presumption in favour of disclosure of all public records (Interview with Wayne Hendricks, 28 July 2005).

Providing adequate resources for the implementation of the PAIA was a challenge to the NIA and the SASS, and also to the DOD. In NIA, both the primary and secondary DIOs were members of senior management with other critical responsibilities. Yet they did not have sufficient staff dedicated to the task of following through PAIA requests. The NIA's primary DIO, Jackie McKay, said that this was in contrast to developed countries he had visited, including the USA and Canada, which have well-resourced units with staff singularly responsible for ensuring effective implementation of the countries' access to information legislation. McKay claimed it was this lack of resources that resulted in the NIA sometimes failing to respond within the stipulated deadlines (Interview with Jackie Mckay on 15 July 2005).

Compliance by the intelligence services with the provisions of the PAIA

Both the NIA and the SASS Directors-General were cognizant of the main requirements of the PAIA, but admitted that their departments fell short of all the requirement of compliance. This appeared to support my thesis that the services were ambivalent about the implementation of the transparency required by the Act. However, with public consciousness about the Act growing, both displayed openness about their services' shortcomings.

Appointment of Deputy Information Officers

Whilst the NIA Director-General, at the time of interviewing (4 August 2005), indicated that the NIA had appointed a DIO in compliance with the provisions of the PAIA, the SASS Director-General said that his organization had not as yet done so. The NIA, accordingly, had also published the name and contact details of its DIO.

The SASS Director-General, Hilton Dennis, indicated on 25 July 2005 that he was considering appointing the department's General Manager for Information Technology as the DIO on the basis that he was the official most aware of the nature of records held by the service, their classification status and their location in the department's various databases.

Manuals

Another mandatory requirement for public bodies was the production of manuals in which they would provide for public information, details about themselves. On 31 July 2002 both the SASS and NIA applied to the Minister of Justice and Constitutional Development, in terms of s 14(5) of the PAIA, requesting exemption from the compilation and submission of a manual. The reasons offered by both departments, whose applications were coordinated by the Ministry for Intelligence Services, was that compliance would compromise their mandates, and jeopardise national security.

On the basis of these terms, the Minister granted the exemptions. Significantly, the 184 other requests for exemptions by other bodies in that period were all turned down (Interview with Marlyn Raswiswi, 4 August 2005). In contrast, the DOD did produce a manual as required by Section 14, which contained a fairly detailed description of records held by the DOD, inclusive of military intelligence records. The manual describes the functions and structures of the DOD, drawing on legislation and the Constitution. It also provides the contact details for the Information Officer, who is the Secretary for Defence, and the Deputy Information officers in the DOD, who total 26. The guide on how to use the Act contains information on request procedures, internal appeal procedures, and fees payable by requesters (Department of Defence, 2003).

The section dealing with access to categories of records held by the DOD is divided in two. The first section deals with categories of records automatically available. These are lists as DOD publications, including the Defence Review of 1998, DOD instructions and polices (an index of which is available on the DOD website), Annual Reports for the years 1997 to 2001, Strategic Plans for the years 2002/2003 and 2004/2005, and information bulletins (an index of which was available on the DOD website). In addition, back copies, some dating from 1913, of various corporate communications publications were available. There were also records available in the DOD archives dating from 1912 when the Union Defence Force (UDF) was established. The manual gives a concise but explicit summary of the information that is held in the Archives. Among other records, the archives preserve the records of all former members of the SANDF, SADF and UDF, dating back to 1912, and containing information on the military careers of personnel (Department of Defence, 2003).

The DOD manual lists the categories of records that may be requested. Their classification, for purposes of the manual, is aligned to the DOD filing system. A concise description of each category of records is provided, and the subcategories listed. For example, Intelligence has the serial number 200. This category is described thus: "the series of records pertains to military intelligence. This includes all military intelligence policies, security of persons, information and facilities; the collection of information through various means; intelligence appreciations, forecasts of threats, intelligence reports and interdepartmental intelligence affairs" (Department of Defence, 2003).

Pertinent to the core business of the DOD is the category of records, Operations, with serial number 300. According to the manual, this series refers to the records on military operations. It covers a wide range of topics including strategic planning and appreciations, order of battle, mobilization and demobilization, conventional and unconventional warfare as well as specific operations; air and maritime defence; search and rescue operations and training exercises; assistance to and cooperation with other institutions and countries. There are thirty one sub-categories of records under Operations. Other broad categories, each of which is broken down into sub-categories are Personnel (7 sub-categories); Logistics (8 sub-categories) and Departmental Management (28 sub-categories) (Department of Defence, 2003).

The DOD manual even lists the Defence Intelligence computer applications, which are described as supporting the intelligence business process of the DOD by providing support throughout the total life-cycle of the intelligence process. The manual contains other information, including a summary of arrangements allowing for public participation in the DOD's formulation of policy. These include the role of the Joint Standing Committee of Defence in inviting submissions on Bills being considered by Parliament, or arranging hearings or workshops of matters of public importance; they also include provision for the public to respond to certain notices in the Government Gazette.

Voluntary disclosure

Both the NIA and the SASS Directors-General were able to account for a degree of voluntary disclosure, another requirement of the PAIA. Both have public websites on the Internet. The NIA since 2001, has for each year, produced a public annual report, and the SASS released its first public report in the form of a Ten Year Review in 2004. Much of the information released by the SASS and the NIA related to their mandates and functions, and their corporate profiles. Information on the NIA website includes the following categories of information, inter alias: the vision and mission; a historical overview; a brief outline of the structures of the civilian intelligence community; oversight mechanisms; the legislative mandate; NIA annual reports; human resources information; corporate events; focus areas of the NIA; the code of conduct for intelligence workers; and contact details. The SASS website had a similar profile and also contained the SASS Ten Year Review. In future, the Director-General indicated, the SASS would consider releasing information about its achievements over the year. In June 2005, the Ministry for Intelligence Services also launched a website, containing among other items, budget vote speeches of the Minister and replies to questions that had been directed towards him in Parliament (Interviews with Hilton Dennis, 25 July 2005; Billy Masetlha, 4 August 2005) .

Information about the services is also supplied in the course of the year to oversight bodies, making itself into the annual reports of the JSCI, and the annual reports of the Auditor-General. Several media briefings had also been initiated by the departments in an attempt to improve public understanding of their roles (Interviews with Hilton Dennis, 25 July 2005; Billy Masetlha, 4 August 2005).

Dennis commented that public disclosure of the records of the apartheid period could be useful in bringing closure to that period. The critical challenge would then be to develop a credible standard for withholding information, a requirement that was a reality for intelligence services. For the citizens of South Africa to have trust in the intelligence services, he argued, there must be sufficient transparency about the intelligence services to generate this.

Dennis also stressed that he had interacted with the heads of several intelligence services, particularly from developed countries, with experience of working in democratic dispensations that included legislation guaranteeing the right of access to information. These intelligence services had indicated to him that being subject to such legislation was not detrimental to intelligence work. At worst they might consider it "a necessary evil", but more usually, transparency was seen as important in gaining the trust of society. Dennis concluded that there was great interest and curiosity among the intelligence services in Africa, about the South African intelligence dispensation, particularly the oversight and transparency elements. He said that he believed that South Africa's example, in this regard, was beginning to influence the way in which several countries saw their duty of accountability (Interview with Hilton Dennis, 25 July 2005).

Reports to the Human Rights Commission (HRC) on requests received

In the interview with him on 25 July 2005, SASS Director-General, Dennis indicated that the SASS had not filed the reports as required in terms of Part 5 of the Act, reporting to the Human Rights Commission on the number of requests and appeals, and how they have been dealt with. The NIA Director-General, Masetlha indicated that his department had met all such obligations (interview with Billy Masetlha, 4 August 2005). In an interview, Dr Leon Wessels, a Commissioner of the Human Rights Commission, admitted that the question of compliance of the intelligence services had not received specific attention from the HRC. The Commission faced a more general problem of a lack of awareness of the provisions of the Act from government departments at all tiers, and did not have the resources to focus on the minutiae of the special circumstances of the intelligence services (Interview with Leon Wessels, 2 August 2005).

Processing of requests

The SASS Director-General, Dennis, indicated that since the passage of the PAIA, the service had received no more than six requests. Almost all were from members of the former liberation movements, who were requesting access to their files. The SASS replied to the requests explaining that it did not have the requested records, if they existed at all, because at the time of amalgamation in 1995, all surviving files from the apartheid era had been placed in the custody of the NIA (Interview with Hilton Dennis, 25 July 2005).

In contrast, the NIA had received 43 requests for access to information requests since 1991. In 2001, it received 4 requests; all were "positively responded to". In 2002, NIA received 6 requests and with the exception of the requests for TRC records that were referred to the DOJ, all requests were "responded to". In 2003, NIA received 12 requests; all were responded to "by either indicating that no information was available on the subject matter requested" or making the information available; there were no refusals. In 2004, NIA received 9 requests, the majority having been submitted by the SAHA on behalf of individuals, and there were no refusals. Up until July 2005, NIA had received 12 requests, again with the majority having been submitted by the SAHA, acting on behalf of requesters, mainly prominent figures in the pre-1994 anti-apartheid struggle. Again, there were no refusals (Interview with Billy Masetlha, 4 August 2005).

Most of the requests received by the NIA were for personal information, from persons who had been anti-apartheid activists wanting access to their own files. The SAHA played a significant role in assisting people lodge their requests with various government departments, intentionally by its own admission to determine the state's capability, knowledge and attitude towards the PAIA. According to the Director-General of the NIA, the nature of the "initial requests", during 2002 and 2003, focused on sensitive records of the TRC, former State Security files (with a very specific National Archives index being submitted to substantiate the request), and information on prominent anti-apartheid activists during the period prior to 1990. A trend with the latter was for SAHA to act on behalf of the requester. The NIA also received several requests, which were duly transferred to other public bodies that it believed

held the records requested. These bodies included the National Archives, the Office of the Auditor-General, and the Department of Justice and Constitutional Development.

Case studies

The two case studies presented below are illustrative of the dilemmas and choices facing the intelligence services in balancing secrecy, in the interests of national security, and transparency. I attempt to present in each case the outline of events and choices made by the security services (NIA and the DOD in the respective cases) in processing requests for records, and the response of the requesters to their refusal of access. These case studies highlight the onus of convincing judicial opinion of the validity of grounds proffered for refusal. They also emphasise how fundamental a principle the right of access to information is.

South African History Archives Trust (SAHA) applications to the NIA and the Department of Justice and Constitutional Development (DOJ) for access to TRC records

Background

On 26 November 2002, lawyers for the South African History Archive Trust (the SAHA), served notice that the SAHA intended applying for an order in the High Court (Transvaal Provincial Division) to set aside the deemed decision of the Minister of Justice to refuse three internal appeals that had been submitted earlier that year. The Minister had failed to respond to the internal appeals within the 30 days stipulated in the Act. SAHA's application to the High Court was based on the fact that it believed that the Minister's deemed refusal was also procedurally flawed. Firstly, the applicant filing on behalf of the SAHA, Hatang had not been provided reasons for the dismissal of the appeals. Secondly, the delay in providing the applicant with decisions was neither fair nor reasonable. And thirdly, the applicant had effectively been denied access to the records requested in a manner inconsistent with the Constitution and the Promotion of Access to Information Act (Founding affidavit to the High Court (TPD) by S. Hatang, 25 November, 2002).

The background to the court application was as follows. On 20 May 2002, the Deputy Director of the SAHA, Mr Sello Hatang, had submitted two requests for access to records to the Department of Justice and Constitutional Development (the DOJ), in terms of the PAIA. One request was for copies of all records in the possession of the DOJ documenting the chain of custody of certain listed TRC records, from the time they were transferred from the TRC in 1999, including records detailing amongst other things, location, physical transfer, control, responsibility, processing, and classification. The second request was for copies of the transfer lists used to transfer TRC records from Cape Town to the National Archives in Pretoria. Hatang has several days earlier sent a letter to Mr David Porogo, DIO in the DOJ, informing him of the SAHA's intention to launch a TRC archive project (Founding affidavit to the High Court (TPD) by S Hatang, 25 November 2002).

On 21 May 2002, the SAHA dispatched a third and similar request to the National Intelligence Agency. The NIA replied in writing to the SAHA stating that the TRC documents were the responsibility of the DOJ and were not in the custody of the Agency. It indicated that they would transfer the request to the DOJ in terms of the PAIA (Founding affidavit to the High Court (TPD) by S Hatang, 25 November 2002).

On 12 August 2002, Hatang received a letter from David Porogo, Deputy Information Officer in the Department of Justice and Constitutional Development (DOJ) advising him the documents that had been requested could not be found. As section 23(3) of the PAIA states that a notice that records cannot be found or do not exist is to be regarded as a refusal of access to the records, the SAHA lodged internal appeals against the refusals with the Minister of Justice and Constitutional Development, on the grounds that Porogo did not seem to have applied his mind properly to the requests to the DOJ, or to the NIA request that had been transferred to the DOJ. Also, SAHA contended, Porogo had failed to adhere to the procedures to be followed in respect of the "deemed refusals". The Act stipulated that if requested records could not be found, the information officer had to provide a requester with an affidavit or affirmation to this effect, spelling out in full the steps taken to find the records or to determine whether the records existed (Founding affidavit to High Court (TPD) by S Hatang, 25 November 2002).

In his founding affidavit, Hatang also revealed that he had received a letter from NIA indicating that its request for records relating to the chain of custody of the TRC records was being granted, and that a copy of the letter had been provided to Labuschagne, the Head of Ministerial Services in the DOJ, on 24 October 2002. The NIA had indicated that there were no security or other concerns about providing access to TRC chain-of-custody records, and had provided such records to the SAHA.

Porogo's replying affidavit was lodged on 22 December 2003, more than a year after the motion lodged in the High Court by Hatang's attorneys. In his reply, he claimed that he had been unaware of the whereabouts of the requested records.

> All my inquiries, as well as all the searches I had conducted or caused to be conducted to find these documents or to establish their whereabouts, came to nought. It was only after a journalist, a certain Mr Terry Bell, had given me information concerning their whereabouts, that I learned that the aforesaid documents had been handed over to Mr Dullah Omar – the former Minister of Justice, who at that time, also held the portfolio of Minister for the Intelligence Services – and that the documents were being kept in Dr Omar's office in the Ministry for the National Intelligence Agency.
>
> Replying affidavit to the High Court (TPD) by David Porogo, 22 December 2003

According to Porogo, his efforts to retrieve the documents were rebuffed by officials in the office of the Minister for Intelligence. They stated that the Minister intended to review the documents in the context of a classification and declassification process, which the Ministry would initiate shortly. This was also rejected by SAHA who questioned how the Ministry for Intelligence could take the lead in establishing a process to determine which records could be made accessible, when the DOJ was the responsible department (Replying affidavit to the High Court (TPD) by David Porogo, 22 December 2003).

In February 2003, the then Minister for Intelligence, Dr Lindiwe Sisulu, established a Classification/Declassification Review Committee (CDRC). The terms of reference of the CDRC were to advise the Minister on the best way forward to deal with the requested documents. The CDRC, after considering the matter, recommended to the Minister that the review and release of the sensitive documents be dealt with as a special project approved at ministerial level. The objective was to review the sensitive documents, and then kept in 34 boxes, according to the exemption clauses contained in PAIA. Any document that did not need protection under such exemption clauses would be released voluntarily into the public domain (Interview with Marlin Raswiswi, 4 August 2005).

The CDRC recommended the establishment of an Interdepartmental Review Committee (IRC) to review the status of the requested records and to consider their release. The CDRC would oversee the process for compliance with the PAIA. According to Porogo, "the CDRC's advices (sic) were subsequently approved by the Minister for the Intelligence Services, the Minister of Justice and Constitutional Development and the Minister for Arts, Culture, Science and Technology" (Replying affidavit to the High Court (TPD) by David Porogo, 22 December 2003).

Effectively the review was to entail the CDRC scrutinizing the contents of each record under question and according to criteria adopted as a standard, making a recommendation on whether to release that record to the SAHA or not. In his affidavit, Porogo stated that the review process got underway on 9 September 2003, after preparations that included the special project being approved by the relevant ministers, the sensitive documents being relocated to the South African National Archives, the IRC being established and its members trained for the task ahead of them, and resources being provided for the task. There were three phases to the process: verification of the TRC sensitive documents; actual review of the sensitive documents; and the oversight process.

The verification process was aimed at reaching certainty that all the records that the SAHA claimed existed, could be accounted for. It was conducted under the guidance of Dr Biki Minyuku, the former Chief Executive Officer of the TRC. He was assisted in the verification by the personnel of the National Archives, as well as personnel who had served in the Records Office of the TRC. Minyuku had been responsible for selecting and handing over

sensitive records contained in 34 boxes to Dr Dullah Omar in 1999, believing the records to be sensitive.

Two inventories were used for the verification. The first inventory had been compiled by the TRC and accompanied the sensitive documents in 1999. A second, more detailed, inventory had been compiled whilst the documents were in the possession of the Ministry for Intelligence Services. According to Porogo:

> All the records that were indexed could be accounted for, save for one file, i.e. "W47", which was titled "List of Informers". According to Minyuku, this file only contained correspondence about a list of informers, but that (sic) such a list never actually existed. Minyuku explained to us that the filing was done according to the Documentation Classification System employed by the National Archives, and that such system did not provide for "correspondence" and that the correspondence in this file was therefore filed according to their predominant titles. Porogo claimed that the IRC's management team was attempting to reconstruct the file, by inspecting the electronic databases and backup discs of the TRC.
>
> (Replying affidavit to the High Court (TPD) by David Porogo, 22 December 2003.)

Regarding the contents of the 34 boxes, Porogo indicated that the majority of records belonged to the category of "Chemical and Biological Warfare", of which a large portion had already entered the public domain as a result of the trial of Dr Wouter Basson, a surgeon in the SANDF who had been imprisoned and tried for running secret projects using state funds, allegedly to manufacture chemical agents to direct against anti-apartheid activists during the apartheid era. Other categories of information related to files on the Steyn Commission, an investigation titled "Pro Jack", the investigation into the murder of Paris-based ANC activist, Dulcie September (where most of the information was originally in French), various TRC amnesty hearings, taxi violence and gun running, where some of the documents were in Swedish, German and Portuguese, and the investigation into the assassination of former

Swedish Prime Minister, Olaf Palme, where the majority of, if not all, the documents were originally in the Swedish language.

Porogo insisted in his affidavits that the actual review of the documents contained in the 34 boxes was conducted by the IRC in accordance with the provisions of the PAIA. He denied assertions by experts supporting the SAHA's attempts to access the documents, that the Protection of Information Act and the MISS had been the basis of his decisions when they were eventually made.

The sensitive documents were reviewed and a summary of each document was made, and captured electronically on a computer database. Porogo indicated that depending on the sensitivity of the information and by applying PAIA, the reviewed documents were "reclassified" according to six categories. Full disclosure (bearing the stamp "declassified") was applied to all information contained in a document bearing this classification status could be disclosed. In the case of documents that were partially disclosed (documents bearing the stamp "declassified"), a masking was applied to portions of information that related to exemption clauses in the PAIA. In accordance with Section 28 of the Act, which dealt with severability, the information not masked, could be disclosed. Documents categorised for no disclosure were those which contained information exempted in terms of the grounds for refusal as stipulated under PAIA, Chapter 4.

Disclosure was provided for in the case of some records, but subject to third-party notification. Information should only be disclosed after third-party consent had been obtained, and until such time the information would remain closed. Finally, there was a category of records whose status was still to be determined. The documents in this category were subject to further classification or verification and would remain closed until clarity had been obtained. Examples were the French records on Dulcie September for which the French had to give permission for disclosure (Replying affidavit to the High Court (TPD) by David Porogo, 22 December 2003).

Porogo stated that the reasons most commonly referred to for not disclosing the category of documents identified for "no disclosure" were the protection of personal and third-party information, as well as the protection of methods, technical and manufacturing details

pertaining to chemical biological warfare documents and the protection of foreign relations between states. He pointed out that, with the exception of those documents requiring translation, and which was underway at the time, the majority of records had been reviewed. The details in Table 1 indicate the results of the categorisation as at 5 December 2003.

Table 1. Summary of classification of TRC records, in Affidavit filed by D. Porogo in High Court (TPD) on 22 December 2003

Reviewed status	**Actual numbers**	**Percentage (%)**
Full disclosure	658	39,07
Partial disclosure	198	11,76
No disclosure	296	17,58
Disclosure, subject to third party notification	20	1,19
Status to be determined pending further clarification	512	30,4
Total	**1684**	**100**

Marlyn Raswiswi of the DOJ's PAIA Unit had been appointed chairperson of the IRC. She elaborated further on the method of work of the IRC, which had consisted of representatives from the SAPS, SANDF, NIA and SASS. The National Archives had provided logistical support during the period that the Committee met, and the actual review took place at their premises. As chairperson, Assisi says that she tried to ensure that there was consensus on the classification that should be accorded a document. Once there was consensus, she as chairperson "would rephrase the reason for the reviewed status, in terms of the PAIA requirements". She indicated that most of the information that had been withheld had been provided to the TRC on grounds of confidentiality. The IRC had completed its work in January 2004, and handed its report to the CDRC (Interview with Marlyn Raswiswi, 4 August 2005).

On being informed of the status of the documents, Hatang was also informed by Porogo's attorneys that the documents could be inspected and copies obtained at the premises of the National Archives. In informing Hatang's attorneys of this arrangement reference was made

to a document titled "Worksheet for the review of the TRC documents", running into 411 pages, and containing a complete summary of all the documents described as "sensitive documents" contained in the 34 boxes. The worksheet contained a brief description, not only of the documents that had been declassified, but of highly sensitive documents that had been classified as not possible to disclose at all, and was itself classified as a "Confidential" document. The worksheet was a document drawn up during the review process for the purposes of the IRC and CDRC. Porogo argued that the SAHA was not by right, entitled to a copy; he was simply making it available to the SAHA to facilitate their ability to understand in greater depth the basis on which the DOJ decisions had been made. Porogo stated that the SAHA was offered a copy of the worksheet to refer to provided it accepted the confidentiality regime of the worksheet (Replying affidavit to the High Court (TPD) by David Porogo, 22 December 2003).

This was rejected by the SAHA, on the grounds that they could not accept a response to a request that was given "in confidence". Porogo indicated that in view of the SAHA's refusal to accept the worksheet on condition of confidentiality, he proposed as a practical approach, that a member of his staff be on hand at the time that the applicant and their attorneys inspected the documents at the National Archives. This was to advise them which particular reason or reasons for non-disclosure applied to particular documents.

In his replying affidavits to the court on 22 January 2004 and subsequently on 25 February 2004, Hatang also took issue with several matters pertaining to Porogo's response to their request. In summary, he argued that it was not apparent what the status of the CDRC and IRC were in relation to the request made by decisions made Porogo, concerning the documents; SAHA felt that Porogo had not exercised his mind independently. Moreover, the form in which the documents were made available (photocopies whereas SAHA claimed that their application was to inspect the records) was unacceptable; SAHA claimed that the lack of access to the original documents made it impossible for it to verify the integrity of the documents (Replying affidavit to the High Court by(TPD) Sello Hatang, 22 January 2004 and 25 February 2004).

Hatang also pointed out several administrative errors in the response provided by Porogo. For example, the reasons granted for non-disclosure appeared to contradict the documents

actually provided, leaving him and the SAHA in confusion as to the status of the documents. In other cases, where the response stated that the applicant was entitled to access certain documents, the documents had not been provided. Hatang also refused to accept that certain records such as a report titled "Progress report on the work of the TRC Investigation Unit" were likely to contain confidential third party information, as was contended by Porogo, and rejected the contention that certain files were being withheld on the basis that "family members" of persons in documents had to be consulted since this was not a ground provided for in the Act. Likewise, another reason cited in the reasons given by Porogo, this time in relation to the masking of sections of an Afrikaans document titled "Final report: USA Dollars advance payment", i.e. that the masking was intended to prevent the embarrassment of a foreigner, was rejected. Hatang pointed out that the Act did not allow information to be withheld on those grounds. Finally, a substantial number of records had been withheld because they contained third- party information; Hatang pointed out that all the Act required was that third parties be *informed* before as final decision was made, as opposed to the DOJ's interpretation that the third parties be consulted (Reply to the High Court (TPD) by Sello Hatang, 25 February 2004).

Lessons from the case study of the TRC records

The case of the 34 boxes of TRC records, as the matter came to be regarded and reported in the media, is a compelling one, deserving of thorough analysis. It cuts to the heart of the matter of how committed the intelligence services are to transparency, and whether they are prepared to uphold the rule of law in implementing secrecy measures. Even though the high court applications and counter-applications were between the DOJ and the SAHA, the Ministry for Intelligence Services was a looming, if not highly instrumental, presence in the unfolding developments. Close scrutiny of the matter raised a number of issues.

One was whether the Ministry for Intelligence Services acted lawfully and in the public interest by prevaricating about the NIA's knowledge of the whereabouts of the records that SAHA had requested access to, and what they sought to conceal by not immediately admitting to knowledge of the whereabouts of the records. McKay's response to the SAHA request – that the records were not in the custody of the NIA and were with the DOJ – suggests one of two things: either poor communication between the Ministry for Intelligence

Services and the NIA, or a deliberate attempt to mislead the SAHA. The NIA letter to SAHA several months later, indicating that the transfer lists could be released, is not easy to understand, given that the NIA had initially insisted that it was not in possession of the requested records.

The timing of the establishment of the CDRC, and the inclusion in its brief, of how to handle the sensitive TRC records created the impression that the Committee intruded on the mandate of the DOJ and, to an extent, usurped its role. That the outcome of the CDRC's work had not been made public, even though the former Minister made a public announcement about the establishment of the structure, could potentially fuel the perception that its main preoccupation was the records, rather than a holistic review of the regulatory environment around secrecy and transparency.

The composition, methodology, and recommendations of the Interdepartmental Review Committee beg scrutiny. Although the committee was "trained" for its task, it consisted of middle-ranking officials who were put in the considerably powerful role of recommending the "reclassification" of documents, some of which had not even been originally classified. Moreover, they made their recommendation to the CDRC, which consisted of a cross section of academics and government officials.

Whether the Internal Review Committee had adequate expertise is also questionable, given the administrative errors and high incidence of reasons given for withholding or masking or refusing to disclose documents, which responses had no basis in the Act. It also appears that the provisions of the Protection of Information Act, 1982 may have influenced the reasons provided for refusal of access to some records.

Although Porogo insisted that the DOJ exercised independent judgment in its decisions about how to respond to the SAHA request, there was certainly a trickle-down effect from the deliberations and recommendations of the IRC. Porogo argued that his objectives in serving on the CDRC were not inconsistent with the objectives of the Minister for Intelligence Services. Raswiswi indicated that even after considering the recommendation of the IRC, the Director-General of the DOJ had further studied the request and taken different decisions to those that had been proposed by the IRC. The SAHA, however, had a clear point in arguing

that there was considerable role confusion, especially when they were given a copy of a confidential worksheet emanating from the IRC for further elucidation as to the reasons why certain documents were not disclosed or only partially disclosed.

The respondents' contradictory affidavits and the fact that their revelations came out only under duress is further because for concern, suggested that they had had knowledge of the whereabouts of the records, from before the time that they made their admission that they had discovered the location of the documents. The decision of the Minister of Justice to accept from Dr Minyuku records which the latter had considered "sensitive", and for the Minister to hold them for safekeeping in his Intelligence Ministry offices, was also a problem. Minyuku probably considered himself to be acting correctly, even patriotically, but one must question the effectiveness of his measure: many of the documents were in the public domain; and copies of others were most likely in the hands of individual researchers and investigators. The Minister's decision to hold the documents for 'safekeeping' rather than dealing with them expeditiously – passing those that begged further investigation onto the law enforcement authorities, for example – created the conditions for concern about their integrity, and suspicions about the motives of the intelligence services in preventing their unconditional disclosure.

The matter of the "sensitive TRC records" resolved only after many months and much wrangling between the applicant's and respondents' lawyers, was settled out of court. In consequence, therefore, there is no court judgment out of which a precedent could emerge. The saga suggested ambivalence on the part of the post-apartheid intelligence services about disclosures of the past. The Director-General of SASS, indicated that he had been in favour of disclosing the secrets of the past during the TRC hearings, especially in relations to South Africa's chemical and biological warfare programme, but that senior former NIS officials had resisted the idea (Interview with Hilton Dennis, 25 July 2005).

In the public eye, neither the Minister of Justice nor the Minister for Intelligence Services was ever questioned by the Cabinet about the handling of the matter in all the time that the dispute about the whereabouts of the documents raged. This silence suggested that there was at least tacit support for their handling of the matter. The failure moreover, of the Cabinet to respond

to the DOJ's stated aim of retrieving the document from intelligence is suggestive of relatively greater influence and power on the part of the intelligence services.

Some of the records contained in the 34 boxes related to the ANC, which could have authored them. The PAIA regulates access to information held by public or private bodies, irrespective of whether the records were authored by these bodies or not. The only relevant factor in determining whether access should be granted or not is whether one or other of the grounds for refusal applies. It is possible that the Minister for Intelligence Services was concerned about certain information being released into the public domain but a more appropriate response was have been to develop clearer policy guidelines on how to handle requests relating to information that had been authored by political organizations.

In 2005, the SAHA approached the NIA with a query and was referred by the NIA to the Ministry for Intelligence Services. The SAHA was making preliminary enquiries about records relating to the "Bible Project", an ANC intelligence operation in the mid-1980s that had been headed by Mr Moe Shaik. During the Hefer Commission of Inquiry into allegations that the National Director of Public Prosecutions, Mr Bulelani Ngcuka, had been a spy for the apartheid government, Shaik had claimed that he was in possession of the "Bible Project" records because he had never received an instruction to hand them to any statutory intelligence body. He later reported in his testimony to the Hefer Commission that he had handed the records over to officials of the Ministry for Intelligence Services (Levy, 2004).

Raswiswi, who had been recently appointed Deputy Information Officer in the DOJ, indicated that the department had received another request for TRC-related documentation; this time around the deaths of the "Cradock Four", four anti-apartheid activists from the Eastern Cape, whose had been killed by apartheid security policemen on their way back from a meeting in the 1980s. Because of this The Director-General of the DOJ had taken the initiative to set up another Interdepartmental Review Committee, which would function along similar lines to the erstwhile structure (Interview with Marlyn Raswisisi, 4 August 2005).

The SAHA's request for access to information about the TRC must be seen in the context of the TRC's experience in trying to uncover the fate of apartheid era records of the security establishment. At the time when it conducted an investigation into apartheid era records, the

TRC's findings were of massive destruction of records, engineered by the state's intelligence agencies, primarily the National Intelligence Service. Alarmingly, even under a new and democratic government, the destruction of records continued in 1994, prompting the Cabinet to impose a moratorium on the destruction of records in 1995.

That no clear guidelines existed for the handling of requests for access to TRC documents, at the time that SAHA lodged its requests, is a matter for concern. The DOJ suggested it was attempting to deal with requests for access within the framework of the PAIA, yet the SAHA suggested that the DOJ was influenced in its decisions by the provisions of the Protection of Information Act, 1982. It would appear that a proactive effort is required to determine a strong legal basis for the withholding of records; further, that proper and intensive training is given to government departments about implementation of the Act; and the status of the intelligence services' classification and declassification powers be reviewed and recast in an unambiguous legislative framework.

CCII Systems (Pty) Ltd vs the Minister of Defence on the release of records relating to the government's Strategic Arms Procurement Package

The second case study is derived from the record of the judgment in the matter of CCII Systems (Pty) Ltd vs MPG Lekota, heard in the High Court (Transvaal Provincial Division) by Justice Southwood during 2002. CCII - the applicant - was seeking an order to direct the respondent, Mosieua Lekota, who was Minister of Defence, to furnish certain records pertaining to the sub-systems to be installed on corvettes ordered by the Department of Defence (DOD) for use by the South African Navy. CCII, a company whose business was the design and manufacture of computer and software systems for the defence industry, contended that it had been wrongly excluded as a tenderer for the supply of the sub-systems, through significant deviations from the lawful tender process. It had therefore instituted a lawsuit for damages against the Minister of Defence, the Armaments Corporation of South Africa Limited (Armscor), and African Defence Systems (Pty) Ltd (ADS).

Some background to the Strategic Arms Procurements Package or "arms deal" as it was commonly referred to, helps contextualise the decisions made by the various role players. In September 1997, the government had decided to purchase various new weapons systems for

the South African National Defence Force (SANDF). These systems included a package for four patrol corvettes for the South African Navy. Each corvette consisted of a hull, propulsion system and a combat suite. The DOD and Armscor had set up two bodies to assist in the purchasing of the corvettes. One was the Joint Project Team, consisting of technical experts, whose task was to assess the various tenders. The other was the Project Control Board, to which the Joint Project Team made recommendations, so that it could make final decisions relating to the award of the tenders.

CCII did not accept the outcome of the tender process, which was that a consortium of German companies, the German Frigate Consortium (GFC), was declared the preferred bidder for the supply of the corvettes. CCII was of the view that the tender process was unprocedural and therefore sought access to the records arising out of the tender process (Interview with Wayne Hendricks, 28 July 2005).

The background to the court application for access to the records under question was that on 15 January 2002, the applicant had made a PAIA request to the Department of Defence (DOD) for records that the applicant categorized under 54 headings. Over a period of almost a year, the DOD, through its Information Committee, made some of the documents available to CCII. (Southwood noted that the applicant did not question the legality of his requests being considered by the Information Committee, and not the respondent), and therefore did not take issue with this factor in his judgment).

In the remaining cases, the DOD claimed that the documents either did not exist, or refused to give access to the documents, citing grounds provided for in the PAIA. In his judgment, Southwood observed that the DOD, in most cases, had not furnished facts in support of its decisions, but had merely quoted from the relevant section of the Act, when arguing for its non-disclosure of a record, apparently in an attempt to comply with section 25(c) of the PAIA which requires that when a requests for access is refused, the requester must be furnished with adequate reasons for the refusal.

The applicant was not satisfied with the reason for non-disclosure and on 22 January 2003, initiated an internal appeal in terms of section 75 of the PAIA. In his appeal he pointed out

the requirement that a public body should consider whether there were parts of the records requested that could be severed, in order to render the records disclosable.

Judge Southwood, in making his findings, placed emphasis on the duty of a public body with which a request had been lodged, to consider the severability of the record. He argued that section 28 of the APIA required the public body to give access to the part of the record that was not covered by a statutory ground of objection, stating that:

> This is of particular significance where the respondent's opposition is characterised by generalised and sweeping objections on the strength of which he seeks to withhold whole documents and groups of document. The applicant's counsel argued that the court should not permit this mode of opposition. I agree. The public body must demonstrate to the court that it has considered each document with severance in mind. It must identify the part of the document which contains the protected material, give a proper indication of its contents and why its disclosure is protected, and permit access to the rest of the document. Unless the respondent discharges the onus of showing that the whole document (or group of documents) is protected, he has failed to establish what part he is entitled to withhold. Having failed to discharge that onus he would have to give access to the whole document.
>
> (Southwood j CCII Systems (Pty) Ltd v MPG Lekota) N.O

Judge Southwood went on to consider the merits of the legal arguments presented by the applicant and the respondent, and those arguments and aspects of the judgment that appear more relevant to the intelligence community are summarised below.

Request for "access to the umbrella agreement for the Corvette"

When the request had first been launched, the Information Committee had refused access in terms of section 36(1) which protects commercial information of a third party, and section

37(1) which protects confidential information of a third party. In the view of Southwood, neither the Information Committee nor the appeal authority had given adequate reasons for the refusal, and neither had considered whether there were any parts of the requested record which could be severed (deleted) because of their sensitive contents, so as to make the rest of the document available to the applicant.

In papers submitted before the court, the respondent introduced a further reason for seeking to protect the record from disclosure, namely section 41, which states that records may be withheld so in the interest or defence of the Republic, or to protect international relations. The judge again pointed out that the respondent had not produced facts in support of using this reason. Even though the respondent had not argued for non-disclosure on the grounds of section 42(2), neither had any facts been introduced that would justify an argument that disclosure of the agreement would be likely to materially jeopardise the economic interests or financial welfare of the Republic or of the government to manage the economy of the Republic or of the government to manage the economy effectively in the best interests of the Republic.

Request for "access to the supply agreement for the Corvette Platforms (Part A) and the Corvette Combat Suite (Parts B and C)"

The Information Committee and the appeal authority had refused information in terms of sections 36(1) and 37(1) of the PAIA, and had relied on clause 26 of the Supply Agreement, an addendum to the Umbrella Agreement, which prohibited the disclosure of any information contained therein, without motivating their reasons.

In his affidavit, the respondent stated that the supply agreement contained commercially and financially sensitive pricing information, relating to the Republic, the contractors and suppliers. In addition, section 26.10 of the Supply Agreement stated that:

> Armscor, the End-User and the Seller will keep confidential all information including specifications, plans, drawings, lists and other data, whether furnished to it in writing or by electronic means prior to the date of this schedule A or after, and which is clearly and conspicuously marked as confidential or

> proprietary. The same shall apply with respect to such information which is not so marked but where Armscor and the End User had clear reason to know that such information was to be kept confidential. Such information shall only be used for purposes under this Schedule A or as may be otherwise agreed in writing by the Parties.
>
> (Southwood j CCII (Pty) Ltd v MPG Lekota. N.O)

Again in respect of the above-quoted clause, the judge pointed out that the request was for the supply agreement itself, and not for the protected information described in section 26.10. He therefore rejected the claim that the Act contained grounds for the refusal of the requested information.

> **Request for access to "all records, agendas and minutes of meetings and deliberations of the Joint Project Team relating to relevant decisions regarding nomination, selection and awarding of sub-contracts regarding the Corvette Combat suite" and "all quotations and offers regarding the SMS submitted to the Joint Project Team by the German Frigate Consortium as received from ADS"**

Here again, the Information Committee and the appeal authority had refused access in terms of section 36(1) and section 37(1) of the PAIA, but had failed to set out any facts in support of these sections. In their affidavit, the respondent stated that the records requested contained information supplied by the applicant's competitor, and that it could not therefore provide this third party information. However, the judge held that the information had aged since it was more than four years after the awarding of the contract; the information was therefore merely of historical interest. In any event, the respondent had failed to provide information that showed that, if the information were supplied in confidence, its disclosure would put ADS or any other third party at a disadvantage in negotiations or competition. Moreover, the judge held that since the quotations had preceded the conclusion of the Umbrella Agreement, they would not fall within the ambit of the agreement's confidentiality clause. And as far as the confidentiality clause was concerned, the respondent had not claimed that ADS or any other party fell within the meaning of "seller" in that provision.

Other requests for access to information

The judge also rejected the Minister's argument for withholding several other records. The Minister had argued refusal on grounds of confidentiality. But Southwood ruled that this did not constitute adequate reasons, in line with the stipulations of the Act. Some of the records that the Minister had refused access to were: all quotations and offers regarding the Strategic Procurement Package submitted to the Joint Project Team as received from ADS; the main equipment list for the Corvette Platform; the main equipment list for the Corvette Combat Suite; all internal correspondence and memoranda concerning these matters within the Department of Defence; and all correspondence concerning these matters between the Department of Defence and the German Frigate Consortium(Southwood j CCII (Pty)Ltd v MPG Lekota N.O).

The judge supported the applicant's argument that its managing director, Richard Young, had since 1992 held the highest security clearance possible, and that all staff of CCII held at least security clearances to the level of "Confidential". The respondent's argument that Young's security clearance did not entitle him to any information and that such information would only be made available to him as required for specific duties assigned to him. The judge held that there was neither a suggestion in the respondent's affidavits that Young or his staff were untrustworthy, nor that the information made available to him would be at risk.

Judge Southwood also rejected two other reasons provided by the respondent, firstly, that the request was vague and unspecified (section 45(b) of the PAIA). This reason was provided in relation to the request for all internal correspondence and memoranda concerning these matters with the DODD. The judge felt that the concept "these matters" had been used consistently throughout the process and in CCII's applications for access, and that it should be possible to deduce what records were being sought through this phrasing. Secondly, he rejected the argument that the work involved in processing the request would substantially and unreasonably divert the resources of the public body (section 45 (b) of the PAIA). The judge held that it was inconceivable that a well-resourced public body such as the DOD had neither an accessible filing system, nor the staff to process the request. Further, he supported the applicant's claim that the respondent's claim that processing the request would

substantially and unreasonably divert the DOD's resources should be weighed against the significant public interest in the matter.

Lessons from the case study

This case study has important lessons for the intelligence services, because it too relates to information that was considered protected in terms of the PAIA, yet found releasable in the Southwood judgment. The Southwood judgment set precedents that will have to be taken into account by all public bodies.

The judgment highlights the need for bodies considering requests, to be able to give adequate reasons if they wish to withhold records from a requester. Since there is a presumption in favour of disclosure, the public body should not merely cite the relevant ground for exclusion on which it bases it decisions, but be able to substantiate its claims about the likelihood of harm through a convincing presentation of facts in support of its argument.

The public body should consider whether there is any information contained in the record requested, that could be severed, so as to make the record available for disclosure. Again, there is a presumption in favour of disclosure, and in the case of CCII vs Lekota, the judge held that there was a duty on the part of the public body to consider the segregability of the record, as provided for in section 25 of the PAIA.

The fact that a document is marked or classified as confidential by a public body, is in itself not sufficient to invoke sections 36 and 37, which respectively provide for refusal on the basis of containing confidential commercial information, or confidential third party information. Again, Southwood specified that this claim would have to be contextualized and properly motivated, and he contended that a record could lose its risk rating that had originally required it to be held confidentially, with the passage of time. Therefore, if wanting to invoke either section 36 or 37 as grounds for refusal, the likelihood of harm, along the lines specified in the Act, would have to be carefully argued by the public body to whom a request had been put.

Similarly, it is not sufficient to argue that the security or defence of the Republic could be prejudiced, even if it is the core business of the public body to maintain the security or defence of the country and the information in its possession relate to this reality. The Southwood judgment, noted that not only is the ground for refusal a discretionary one, but that the case for non-disclosure would have to be motivated.

The judgment, further, suggested that arguing refusal on the grounds that a request is frivolous or vexatious, or would involve a diversion or resources, should be used circumspectly; in the case of CCII vs Lekota, the judge argued that the DOD in all likelihood had the resources to process the request of the applicant, and that the matter was of sufficient public interest to warrant the resource that such a request might need.

Lastly, the Southwood judgment suggested that a public body, in considering refusal of a record, should apply all resources necessary to develop legally sound arguments at all stages of the process: when a request is first presented, during the internal appeal process and if the matter is taken to court. It appeared that raising additional grounds for refusal, in particular the grounds that disclosure could prejudice the defence and security of the Republic, invoked a cynical response by the judge, who went on to order disclosure.

The Southwood judgment can be considered as a very strict interpretation of the PAIA's grounds for refusal, but it was and is a real factor in the field of legal interpretation. The DOD was obliged to accept and implement the findings of the judge, despite the self-imposed strictures of secrecy and confidentiality it assumed were sufficient to shield records that it held from disclosure to a requester.

Concluding remarks

The experience of the intelligence services in the implementation of the PAIA was uneven, a situation not unlike that in many other government departments. The most basic requirements, the formalization of a policy and the appointment of a Deputy Information Officer(s) were still being finalised by SASS as at August 2005. The SASS had not received a large number of requests in terms of the PAIA – only six since 2001, according to the Director-General. Its own efforts towards disclosure of information were self-initiated and do

not appear to have been motivated primarily by the provisions of the Act. There has been greater pressure on the NIA to respond to requests, numbering from six to twelve per year. The NIA claims that it has, by and large, sought to disclose the records and that its refusals were based on reasons provided for in the PAIA.

The Ministry for Intelligence Services has played an ambivalent leadership role in relation to the PAIA. In the first place, it appears to have supported, if not coordinated, the applications of the NIA and SASS, for exemption from the section 14 requirement for public bodies to produce a manual. The grounds on which the exemption was requested were very vague, and suggested that there had not been in-depth policy debate before the application for exemption was made. By way of contrast and comparison, a policy was adopted at the highest level in the Department of Defence and the manual produced by the DOD provides for categories of intelligence records that may be requested from that body.

One of the most telling indications of the intelligence services' approach to the PAIA came in the form of the response to the SAHA's application for access to sensitive records that had been transferred from the TRC to the Minister of Justice, who was also at the time (in 1999) the Minister responsible for the Intelligence Services. The NIA transferred the request to the DOJ (which had received a similar request directly from the SAHA). The DOJ became embroiled in a months long behind- the- scenes battle to wrest control of the documents from the Ministry for Intelligence Services, in order to process the request.

The matter of apartheid-era records is very much alive and in the public consciousness. A study of the records requested by SAHA from the NIA reveals that most requesters have shown interest in the records held by the state about themselves. There is, seemingly, a need for the intelligence services to devise a proactive process around declassification, and to provide information about the records available to the public. This will avoid these services becoming involved in time-consuming exercises of searching for records, and possibly, expensive litigation when disputes around access arise. In addition, there is a need to review the legal basis of the procedures and criteria for classification. The following factors, all lacking in the case of the interdepartmental review process should be addressed in the regulatory framework: the criteria for classification should be aligned with the PAIA; there

should possibly be restrictions on who has the authority to classify records; and there should be stricter oversight over classification procedures.

The Southwood judgment arising out of the dispute between CCII Systems (Pty) Ltd and M.P.G. Lekota, the Minister of Defence, brought home several realities. The main lesson is that the marking of a document as classified, carries no legal weight in the consideration of a request for access to that record. This underlines the point that had been made by van Schoor, one of the primary drafters of the PAIA (Interview with Empie van Schoor, 23 August 2003). All that matters is the applicability of the grounds for refusal as contained in the PAIA, which must be appropriately cited and motivated. The temptation to exclude whole records is also a risky option, since in addition to the presumption in favour of disclosure, there is a requirement in the Act that the body to whom a request has been put, should if it believes disclosure to be appropriate, demonstrate that it has applied its mind to severing those parts that contain the protected information, and releasing the rest.

These findings have important implications for the intelligence services, which are subject to the Act. Policy making is a dynamic and responsive process. The intelligence services have as yet consciously to define their responses to the Act. An overarching framework is absent, and the lessons from the countries reviewed differ from one to the next. Policy makers in government, the courts, oversight bodies, and role players in civil society, are faced with the challenge of developing policy options that reinforce the constitutional principle of access to information, while taking care not to erode the ability of the intelligence services to perform their constitutionally and statutorily defined roles.

CHAPTER EIGHT

ANALYSIS OF THE RESEARCH RESULTS

Introduction

The primary aim of this study was to explore a policy framework for determining what information about or held by the intelligence services, should be made available to the public. Althyough policy for implementing the Promotion of Access to Information Act, 2000 (PAIA) was the focus, broader issues of public accountability, governance and democratic control of the intelligence services also arose in the research. The study raised challenging policy questions generated by the access to information provisions of the Constitution and the legislation. Among these questions were: who should have the authority to classify information and in terms of what thresholds or standards; how should the records of the apartheid intelligence services be preserved or handled, especially in the context of processes to encourage disclosure about human rights abuses; what safeguards should be in place to ensure that the declassification or classification of information is in the public interest; and lastly, what role can civil society and even policy makers consciously play in determining policy around these and other questions?

It was found that the secrecy under which intelligence services conduct their business is a worldwide phenomenon which has characterized authoritarian as well as democratic political systems (Lustgarten & Leigh, 1994; Hodess, 2003). Notwithstanding the introduction of the concept of 'human security' as a strong philosophical underpinning in the debate on national security in the period after the Cold War, global conflict and insecurity have persisted (Cawthra & Luckham, 2003). As the literature review (Chapter 3) revealed, official secrecy moreover, has been a problem confronting even liberal democratic states, over a long period of time (Mathews, 1978; Robertson, 1999). In South Africa, what distinguished the secrecy of the period prior to 1994 from that of the post-apartheid period was that the earlier variant was integrally linked to an undemocratic, racially exclusive constitutional order, and served to

undermine human rights (Truth and Reconciliation Commission Report, 1998). The post-apartheid Constitution makes provision for a fundamental right of access to information, to which all other legislation and regulation is subordinate (Currie & Klaaren, 2002; Levy, 2004).

In the post-apartheid context, the overarching factors driving the intelligence services' resort to secrecy are both the perception of threats to national security, and their awareness of a constitutional obligation of a degree of transparency. Because the existence and role of the intelligence services is upheld in law - in fact, it is upheld by the Constitution of the Republic of South Africa, 1996 which makes provision for the President of the Republic to establish intelligence services (section 209) and spells out the principles that should guide their conduct (section 198) - the study sought to explore how the constitutional imperatives of access to information, and legitimately constituted intelligence services performing a constitutionally legitimate role, could be reconciled.

Chapter 4 of the study, which explored the roots of official secrecy in South Africa, demonstrated that secrecy was a significant factor in the system of political governance in South Africa throughout the twentieth century (Mathews, 1971; Bindman, 1988; Geldenhuys, 1984). Yet a study of the emergence of the country's democratic political dispensation, and the emergence of the country's post-apartheid intelligence agencies, shows that secrecy remained a factor and an instrument of governance during the transition and when the new intelligence dispensation was established. For the intelligence services, the ground was therefore set for a complex relationship to the requirements of secrecy and transparency, as the contradictions in their posture tended to suggest.

Managing intelligence information in the transition

The entrenchment of democratic principles arising out of the negotiations for a democratic political dispensation in South Africa, created the basis for a new culture of accountability and transparency over intelligence. The new services faced many challenges but oversight bodies appeared to be satisfied with their performance.

Even though the intelligence services operated in terms of new legislation and repealed in entirety the old legislation, there were significant continuities with the old. During the period of tenure of the Transitional Executive Council agreement was reached that the administrative systems of the National Intelligence Service as well as their regulations would be used initially used, and revised within a short period of time. In reality the review happened very slowly, and the new services inherited and came to operate in terms of the arcane regulations and systems of the old order (Interview with Moe Shaik, 17 October 2003).

The introduction of a constitutional right of access to information rested uneasily with laws and administrative instruments designed to protect classified information. The latter was one of several vestiges of the apartheid era, that included the Protection of Information Act, 1982, and the Minimum Information Security Guidelines, a Cabinet directive that gave officials authority to classify documents on grounds of protecting national security, and thus to restrict public access to the information contained in the documents (Currie and Klaaren, 2002).

Implications of the key issues in the literature

The constitutional basis for access to information in South Africa, as discussed in the literature review (Chapter 3), has been the subject of considerable academic literature. Analysts have studied the implications of the right of access to information in a variety of areas of social life such as employer-employee relations, health, trade practices, criminal investigations and trade matters. It is relevant to raise several issues that emerged during the literature review at this point, as they help to put the discussion on policy options in perspective. The first is whether a value judgment can be attached to secrecy or transparency, whether either of the two can be regarded as good or bad for governance, especially of the intelligence services (Bok, 1982). The review suggested that while the matter is a complex one, there is an overwhelming case to be made for more, rather than less, corporate transparency. One of the reasons is that modern societies have developed a greater intolerance of the secrecy that so characterised bureaucracy in earlier times (Mathews, 1978). In the case of intelligence services, which tend to operate under conditions of secrecy, policy makers should strive to ensure that this condition does not become self-serving and habitual, and is only exercised where harm might result from the alternative approach of transparency.

Robertson (1999) asserts that freedom of information legislation can serve as a constraint on open government, because it places on the public the onus of requesting information, as opposed to placing on governments, the responsibility for disclosure. He argues that freedom of information legislation is little more than a revised system of information management, which continues to favour the elite classes in society. In any case, such legislation rarely offers access to critical information about policy making, and is weighted in favour of facilitating access to personal files.

The warning Robertson (1999) issues needs to be placed in context. Granted, restrictions may be placed on access to records of policy-making structures, including a blanket exemption on all Cabinet records. Indeed, taking the example of South Africa's Promotion of Access to Information Act, 2000, the extent of the exemption clauses is wide-ranging. But in societies where access to public records has been absent, and that space filled instead with repression, the right of access to information is a meaningful victory; South Africa is such an example. The right of access to information moreover is entrenched in the Constitution as a fundamental right, and the legislation which details the exercise of this right, also makes provision for voluntary disclosure of information, so as to promote a culture of transparency. The question is whether public bodies, especially, do enough to promote knowledge about their mandates and functioning, or rely exclusively on the legislation as the basis to satisfy public curiosity or demands for information. Here, one must look at the role of manuals in promoting such knowledge: whether there is enough pressure on public bodies to produce and disseminate them or indeed to spread knowledge and information in other, perhaps more appropriate forms. Where Robertson (1999) does have a valid point, is in arguing that other mechanisms of governance promoting accountability should not be abandoned, since access to information legislation on its own will not deliver open, transparent and accountable governance.

The literature review also showed that access to information is a universally acceptable principle increasingly played out in a world where globalization, rapid technological development and an information explosion challenge traditional notions identity, the impenetrability of governments' information systems and the viability of the secret intelligence organization (Lipinski, 1999; Hodess, 2003). Communications technology has developed to such an extent – there is a myriad of satellite, digital and electronic possibilities

- that most governments admit that they cannot guarantee that information they develop, store and communicate, is not vulnerable to unauthorized access. This affects the durability and effectiveness of secrecy regimens that governments might have in place, and calls into question the considerable funding that must go into physically securing information systems and personnel entrusted with information security. At another level, another factor affecting the effectiveness of secrecy systems is globalization, and the growth of multinational governmental and private entities. This has given rise to a global scenario where identities are increasingly cast in transnational terms, rather than mere citizenship of a country of birth.

The literature noted that the debates around national security and the governance of the security sector, had raised important issues, both internationally and in the developing world, in the period following the end of the Cold War (Le Roux, Rupiya & Ngoma, 2004). Effective governance of the security sector was increasingly measured in terms of criteria such as civilian control of the security services, effective oversight through Parliament, and transparent and effective management. But Cawthra & Luckham (2003) warned of the challenges of security sector reform in Africa, owing to the dynamics of conflict, many of which had complex root causes.

Their writings resonated with the concerns expressed by Buzan, Waever & de Wilde (1998) about the securitization of social and political issues. By and large, placing issues in the security realm, marked a failure to address them in the more normalised world of political engagement. As much as war represents a failure of politics, the resort to secrecy – particularly if it is excessive – by the state, is an indication that the normal course of politics has failed. This therefore drives society back into that dark abyss of unaccountable and authoritarian state conduct.

Finally, the literature revealed a relevant concern, about the handling of official records in times of transition, and under conditions of political normality (Hayner, 2001; Simpson & Posel, 2002; Hamilton, et al.) During periods of transition, the record is highly contested; one group seeks to access it to confirm its fears of the worst excesses, whilst the other may seek to destroy it to eradicate evidence of its shameful past. Yet, the record is representative only of officialdom's version of reality: in the context of the intelligence services, only what the state perceives as a threat to security will be recorded, to the possible exclusion of the people's

voices. Of equal concern is the fact that records are often so inaccessible to the public, in a way existing only for the public official or researchers who may come to know of their existence. It is precisely for this reason that public declarations of the information held by the state, and the existence of conditions for easy retrieval and access to such records becomes so important. There is a very compelling argument for intelligence records to be available for such scrutiny so that they are never again erased from memory in the way that they were under apartheid, nor tampered with so as to distort the account of history.

Interpreting the interview results

The study found that there has generally been a capacity problem concerning the implementation of the Promotion of Access to Information Act (Interviews with Verne Harris, 1 September 2003; David Porogo, 27 August 2003; Leon Wessels, 2 August 2005). The study also found that there is generally a positive attitude towards disclosure of information about themselves by the intelligence services, as evidenced by their voluntary publication of information about themselves through promotional material, the setting up of websites by the NIA, SASS and Ministry for Intelligence Services in recent years, and responsiveness to public queries through the media and in parliament (Interviews with Hilton Dennis, 25 July 2005; Billy Masetlha, 4 August 2005). The heads of the services argued however, that in terms of the law, they had a duty to protect the identities of members and sources of information, and also the operational methods they employ. They cited the Intelligence Services Act, 2002 as the source of this duty. Qunta (2004) confirmed that the law did place such a responsibility on the shoulders of the intelligence services heads, and that the international experience indicated that this was not unusual. Steytler (2004) argued that strategies, consistent with all constitutional aspects of the law, will have to be found to deal with such scenarios in future and proposed that the creative exercise of mandates be exercised to ensure that neither the mandates of the intelligence services nor their accountability to the public, is undermined.

Up until August 2005, the intelligence services had not enjoyed strong executive leadership in regard to the implementation of the PAIA. One of the two services, SASS had not appointed a Deputy Information Officer (DIO), as required by law, and both services, with Ministerial consent had applied for exemption from the section 14 requirement to approve a manual

(Interview with Hilton Dennis, 25 July 2005). Since receiving the exemption, which expires in 2008, there have been no attempts to consider what information should be contained in a manual, or a case could be made for the further exclusion of the services.

Concerning requests for access, NIA was under greater pressure than SASS to respond to requests than SASS, most of them being requests for access to personal information files. Most of the requests were granted, but the DIO indicated that a lack of adequate resources, mainly adequately trained personnel, had resulted in delays in responding to some requests (Interview with Billy Masetlha, 4 August 2005).

The case of the 34 boxes of TRC records cut to the heart of the matter of how committed the intelligence services are to transparency, and whether they are prepared to uphold the rule of law in implementing secrecy measures. It demonstrated also that the matter of apartheid-era records is very much alive and in the public consciousness. The Ministry for Intelligence's refusal to openly admit knowledge of the whereabouts of the existence of the requested had a disturbing ring of dishonesty to it. A year after the access to information request lodged by SAHA, it emerged that the records had been in the offices of this Ministry all along. The SAHA was unhappy with the grounds for refusal given in some cases, arguing that they were not provided for in the PAIA but were more in line with the Protection of Information Act, 1982. Moreover, they claimed that the Ministry for Intelligence had influenced the DOJ in developing a response to the request.

This conclusion is not well-founded, and the cooperative approach to considering the status of records, should not be rejected in principle. In fact, in its own submission to the CDRC, the SAHA proposed an audit of records held by the security services that dated to the pre-1994 era, and a process of declassifying them subject to the provisions of the PAIA. In the case of CCII Systems (Pty) Ltd v MPG Lekota, Judge Southwood took note that a committee had been involved in advising the DOD and the Minister as the appeal authority, on appropriate responses to the applicant's requests. He noted that the applicant had no quarrel with this internal process, and thereafter appeared to accept the given status of the committee as a recommending body, in the processing of requests to the DOJ. Marlyn Raswiswi of the DOJ indicated that her department is still receiving requests for the release of TRC records (Interview with Marlyn Raswiswi, 4 August 2005). There appeared to be a need for the

intelligence services to devise a proactive policy around the declassification and to provide information about the records available to the public.

The utilisation of the PAIA in South Africa has largely been confined to organized NGOs, at some cost to themselves. Knowledge of the Act among the public seems to be limited, and the low levels of literacy in the country suggest that it will be some time before members of the public make full use of it (Interviews with David Porogo, 27 August 2003; Verne Harris, 1 September 2003; Leon Wessels, 2 August 2005).

The intelligence services of South Africa cannot escape their constitutional obligations towards providing the public with access to information about their role and aspects of their functioning. There is a compelling historical basis for this, namely the role played by the intelligence services at the height of the apartheid era, of upholding that system. The generalized cloak of secrecy under which South Africa's security establishment functioned contributed to the institutionalized assassinations, harassment and detention without trial of thousands of South Africans (Truth and Reconciliation Commission, 1998).

It would be in the public interest therefore, for the intelligence services to be expected to engage in maximum disclosure. Institutionalising the production of their public annual reports could be one means of achieving this. Oversight bodies such as the JSCI, the Inspector-General and the Auditor-General have challenged the intelligence services on areas that must be reported on as a matter of course (Interviews with Wallie van Heerden, 21 October 2003). The principle that secrecy should not be used to cover up embarrassments or inefficiency has in the views of these bodies, been reinforced by their insistence on the disclosure of information.

There was a strongly prevalent view in the literature, and among those interviewed during the study, that the Protection of Information Act, 1982 should be reviewed with the view to ascertaining whether South Africa needs legislation promoting secrecy. There was also a remarkable convergence in the interviews on the view that the intelligence services had a duty to respect the constitutional foundation of their establishment, and find ways in which to give expression to the public's right of access to information (Interviews with Tertius Geldenhuys, 7 October 2003, Hilton Dennis, 25 July 2005; Billy Masetlha, 4 August 2005). The

respondents recognised that the key to clarifying uncertainty about what information should be disclosed and what information protected from disclosure, was to clarify what interests were under threat in South Africa. My interpretation of this favourable posture is that it represents a possibility for collaboration on the part of oversight bodies, the Executive, the intelligence services and civil society on a consensus position in this regard.

Other countries' experiences

Helpful in exploring options for the management of information in societies undergoing transition was the literature which discussed the contested records in the transitions towards democratic forms of governance (Hayner, 2001; Posel & Simpson, 2002). In South Africa, this was exemplified in the experience of the TRC that uncovered the mass destruction of tons of documents by the authorities in the years immediately prior to the end of apartheid. This suggested that the apartheid security forces were acting under Executive instruction to eradicate traces of their role in the repression of anti-apartheid opponents. Truth commission processes in other countries such as Chile and Guatemala, also revealed evidence of records being destroyed (Hayner, 2001). In some instances, gaining access to the records of a third country proved successful in obtaining information that could be used by truth commissions in understanding the role of security forces. The truth commission in Guatemala for example, was especially successful in petitioning the USA government for access to records that would shed light on its relationship with the regime that had been responsible for the deaths and disappearances of many Guatemalans. Truth commissions have generally reinforced the need for post-transitional authorities to establish transparent systems of managing official records, so that the integrity of "official memory" is preserved and made available to the public (Simpson & Posel, 2002).

Comparing and contrasting the experiences of other countries with access to information legislation, was also useful (Rankin, 1986; Adler, 1991; Lustgarten & Leigh 1994; Hodess, 2003). It was found that the principles framing access to information are more or less universally found in democracies. Based on an understanding that citizens particularly have the right to information held by their governments, the principles include the need for maximum disclosure to the public of information held by the state; the need for public bodies to voluntarily disclose information rather than rely on requests for access to promote

openness; a limitation on grounds for refusal in response to requests for information; and an inexpensive and accessible system for the processing of requests. There were significant similarities in the grounds for refusal of access to information, including the preservation of national security, the protection of privacy, the protection of trade secrets or commercial information or information relating to the economic interests of a country, the protection of information relating to criminal investigations underway, and information that relates to policy still undergoing formulation. As in the case of South Africa, all these grounds for refusal were contained in the access to information Acts of the USA, Canada and India, the countries compared (Rankin, 1986; Hazell, 1989; Adler, 1991; Martin & Feldman, 1998).

Contrasting the experience of transparency and access to information in post-apartheid South Africa with that of other countries highlighted the fact that there is no single formula for balancing secrecy and transparency. Not all countries' intelligence services find themselves subject to the access to information legislation. In India, the intelligence services are expressly exempt from the provisions of their countries access to information laws. Although not sampled in this study, it is worth mentioning that this complete exemption applies to Australia too, notwithstanding the fact that there is a strongly rooted culture of access to information in that country. In the USA and Canada, the intelligence services are subject to freedom of information legislation (Adler, 1991; Rankin, 1986). In South Africa the intelligence services have been temporarily excluded from the application of provisions requiring them to produce manuals. Yet other countries – Canada is an example – produce detailed and extensive manuals. Legal challenges by the public are often the means for extending space for the application of such acts. What is probably of greater significance is the political culture in a country, and the extent to which other mechanisms of oversight are available.

Policy recommendations

The approach of Lee (1991) is particularly pertinent from this point onwards in the chapter. In discussing the methodology for the study (Chapter 2), I have pointed out the need for policy to relate to real challenges and to attempt to reconcile the interests of various concerned parties. If the mandate of the intelligence services is to identify and report on potential threats to the security of the Republic, the starting point in an information

management policy is for the intelligence services to make an assessment of what institutions, individuals and practices, face security risks.

The basis for determining what should be protected is the Constitution (Levy, 2004). The Bill of Rights is unequivocal about the fundamental rights to which all who are subject to the Constitution shall have access: these rights include the right to life, the right to privacy, the right to freedom of expression, the right to work, and the right of access to information. In drafting the legislation under the new constitutional framework, these fundamental principles have been taken into account.

Currently, most of the information created and held by the intelligence services is routinely classified as being "Confidential", "Secret" or "Top Secret". Moreover, the Minimum Information Security Standards (MISS) gives licence to officials outside the intelligence services to classify information in their possession, with the intention of limiting its disclosure and distribution. There is very little oversight over this process, with the result that information that may not warrant the protections afforded it, is beyond ordinary public scrutiny (Klaaren, 2002). There is a serious need to establish what information is being given security classifications by all public bodies, and to determine whether this occurs as a matter of habit and convention, or because not protecting the information places the state at risk in any way. This was not a focus of my research, and would make for a fascinating study, provided the challenges of confidentiality that an analyst placed in this position would face, could be overcome. This is probably an example where an interested client would have to commission and support such research in order for access to the relevant data to be obtained (Lee, 1991).

Security classification amounts to little more than placing a stamp on a document, and is effective only in as far as providing a deterrent to officials to disclose information thus designated and stamped. Information whose disclosure could pose serious risks to national security (to use one of the exemptions as an example), calls for serious physical security measures, and these should readily be afforded. If disclosure of the identities of agents and sources of information could place their lives at risk, similar protection should be afforded, as should be the necessary penalties to those who violate the requirements of confidentiality.

Another reality that needs to be taken into account when assessing the de facto impact and use value of the intelligence services' classifying records at varying levels of secrecy, is that technology has developed to such an extent that most governments admit that they cannot guarantee that information they generate and communicate is not highly vulnerable to unauthorised disclosure (Lipinski, 1999). Consequently, tremendous resources are spent on securing the information systems of government. No longer is preventing unauthorised disclosure a matter to be regulated by law and providing the physical infrastructure to prevent the leakage of written records; there is a myriad of satellite, digital and electronic transgressions that are now possible, and governments may lose highly sensitive information to other parties without even realising it. Moreover, the Information Age has given rise to a situation where identities are cast in post-national terms, and where loyalties proceed along other interest lines, including economic. Technological advances need to be taken into account when formulating a comprehensive strategy for the classification and declassification of information.

Intelligence services should recognise that there is a massive explosion of information and that they could be utilising technology and "mining" the extensive data banks that can be accessed without risk. Recognising that other states need information, and entering into partnerships with them to share intelligence, rather than competing with them in the Cold War paradigm, is probably a more beneficial approach than is currently employed by many intelligence services (Steele, 2001).

If there is still scope in the South Africa dispensation for the protection of information, the question that arises is whether there is scope for the Protection of Information Act. The aim of the Act is "to provide for the protection from disclosure of certain information". Apart from the wide range of parties to whom such unauthorised disclosure may not be made, the Act spells out the scope of such information, which by definition includes information concerned with the work of any "prohibited place", i.e. any defence installation being used or occupied by or on behalf of the government, information concerning any matter being dealt with by the intelligence services, and any secret official code or password or any document, model, article or information used, kept, made or obtained in any prohibited place.

In the most general of senses, the existence of this legislation is something of an anomaly when considering its co-existence with legislation guaranteeing the public access to information held by the state. It has been argued that the Protection of Information Act, 1982 is in conflict with the spirit conveyed by the Promotion of Access to Information Act, more especially because it had its origins in the apartheid days and its rationale was to prevent access to information by "hostile organisations", defined as organisations declared by or under any Act of Parliament to be unlawful, or any association or movement of persons or an institution declared as a hostile organisation through a promulgation of the President. This assertion however needs to be interrogated, in the light of the fact that the Act does provide for a number of mandatory exclusions, which can be invoked to reinforce secrecy in a number of statutorily defined instances.

There have been strong calls for the repeal of the Protection of Information Act (Currie & Klaaren, 2002). I would argue for a more realistic approach. The PAIA cannot achieve the object of protecting information, or that of imposing penalties on those who do. The MISS has been criticised for being without statutory force. Without anticipating the outcome of a public debate on what information held by the state requires protection, a number of principles can be considered to resolve the question of whether there should be legislationwhich aims to protect certain information. First, the debate should not be confined to the security services but should be wide ranging in scope and sponsorship, and take into account the concerns and value propositions of the full range of policy actors on whom the debate will impact, including non-governmental organisations, oversight bodies, and the Executive (Lee, 1991).

Next, in keeping with the spirit of the Constitution, the debate should be framed with the constitutional principles of access to information, and the reasonable limitation of this right, in mind (Currie & Klaaren, 2002). And given the historical context in which South Africa is operating, protection to statutory information should be defined to include a protection from the state abusing, manipulating and destroying information for its own ends; in other words, it should not only be individuals and organisations, but the State, which in terms of this new paradigm, could be deemed culpable for violating its duty to protect the information it is responsible for (Coliver, Hoffman, Fitzpatrick & Bowan, 1999);

Last, it is probably advisable that espionage (as an offence committed by states with intentions hostile to South Africa's interests) should be clearly defined as a separate offence; even then, in light of a paradigm of sharing information, the actual content of the crime of espionage should be reconsidered (Mathews, 1978).

Principles for the classification and declassification of information

The security forces, particularly the intelligence community, currently classify virtually all information they produce along the lines indicated above. A more proactive approach to the desensitisation and declassification of information on the part of the security services would most likely result in a less adversarial role between a public seeking to gain access to information ordinarily regarded as too secret to share by those who believe they are protecting that information in the interests of national security.

The purpose of a well regulated system of classification and declassification would firstly be to ensure that there is a uniform system for the safeguarding of official information whose unauthorised disclosure could threaten the country's security; secondly, it would ensure that original criteria for withholding information from public knowledge would be routinely reviewed with the intention of making such information publicly available once its disclosure posed no further threat to the country's security.

The legal framework that has historically pertained with regards to state information has been decidedly restrictive. Modelled on British legislation, South Africa, from 1910, was subject to the Official Secrets Act, which provided for severe mandatory penalties for disclosure of state secrets. This was followed by the Protection of Information Act, which if read in conjunction with other legislation, reinforces the culture of penalties for the disclosure of secrets. Important issues of accountability of governmental accountability, of who defines what is legitimately to be withheld as secret or confidential and what checks and balance exists over how officials exercise diligence in their management of information, and of ensuring that the public is sufficiently informed to be assured that government is acting in their best interests, must be debated if a balanced approach to classification of official information is to emerge.

Secrecy on the part of government is provided for in the PAIA exemptions. There are costs to secrecy, including that of physically protecting secrets, the danger of losing public confidence through non-disclosure and the limitation on input and debate; furthermore secrets are vulnerable to leaks which can have untold consequences.

Several concepts can probably be incorporated into a policy framework for classification and declassification. First, government should provide a statutory basis for the secrecy system with clear standards of what is to be classified, by whom, and in terms of what prescribed procedures. Any new legal framework for classification and declassification should be aligned to the PAIA. Given that the PAIA is concerned with effecting disclosure rather than providing a basis for the protection of information, there are grounds for legislation to protect and classify information. The legislation should link the authority to classify information to the degree of classification required. As suggested by Halperin & Hoffman (1977), possibly only designated office-bearers such as the President, Ministers and heads of department should be entitled to classify information as Top Secret, whereas lower level officials should not have such authority, unless it is specifically delegated to them. Government should also consider whether all national departments and provincial and municipal authorities should have authority to classify information. This would be based on a risk management approach. And furthermore, when classifying information, government officials should be able to describe how each piece of data could be a threat to national security, and indicate the time frame for the restriction.

If legislation is effected to provide for the classification and declassification of records, it should incorporate the concept of a life cycle for secrets, i.e. the notion that in the management of information, its sensitivity may reduce over time and thus the need to expend resources on its physical protection. Classification, moreover, should not be effected to conceal violations of the law, inefficiency or administrative error; neither should it be used to prevent embarrassment of a person, organisation or agency, or to withhold basic scientific research information not clearly related to national security. Nor should classification be effected to conceal previously declassified information, as the danger of arbitrary classification can readily set in. Lastly, uniform national standards for declassification should be set, and implementation monitored through an appropriate oversight body.

Various scenarios requiring policy on classification and declassification

In addition to the broad principles outlined above, the study has suggested that policy options for the protection of, yet simultaneous access to information, in a variety of scenarios should be explored. I enumerate several of these scenarios below.

Records concerning the day-to-day operation and mandates of the intelligence services

The study has taken as a given the reality that the intelligence services are subject to the Promotion of Access to Information Act, 2000, notwithstanding the fact that there are countries (e.g. India and Australia) where the intelligence services are completely excluded from the ambit of those country's access to information laws. There is strong public opinion against the security and intelligence services operating outside of the ambit of the PAIA, which in any event, is legislation giving effect to a constitutional requirement. I therefore dismiss the possibility of excluding the intelligence services from the ambit of the Act, and have taken the approach of reflecting on how the intelligence services can act within the framework of the PAIA.

The first scenario to be considered, therefore, relates to the day-to-day functioning of the intelligence services. In gathering intelligence - domestic and foreign - and in fulfilling their counter-intelligence responsibilities, the intelligence services author, and come into possession of significant amounts of records. As suggested by the Director-General of SASS (Interview with Hilton Dennis on 25 July 2005) a useful distinction can be made between corporate information and intelligence information. Corporate information would include information about the administration of the services, including their legal mandate and mission, their human resources management, their policies and procedures, their finance, assets, and transactions with corporate and services structures. Some of this information may be considered worthy of protection by the services, and should well enjoy protection, provided that the services are able to motivate clearly what harm could come to the country if the information is released. To avoid inconsistencies in dealing with requests, the intelligence services should consider the institutionalisation of public annual reporting, with a minimum base of information on all the above corporate areas being provided. Simultaneously, they

should seek legal opinion on whether the information that they seek to protect, can be accommodated within the provisions of the PAIA.

Voluntary disclosure is in fact, a further requirement of the PAIA, and the intelligence services, in so releasing information through their public annual reports, would be giving effect to the relevant provisions in the Act. The social benefit is that they would contribute to a broader understanding of the intelligence services' functioning, and serve to demystify a matter that is little understood by most people. The challenge in a country such as South Africa is to reach out to the broadest mass of people in such acts of voluntary disclosure. Given the high poverty and illiteracy levels, creative grassroots approaches, such as the use of the radio, and visiting local communities to explain these matters, could be made.

The second category of information - intelligence information - can probably be further broken down into categories such as operational information and intelligence reports. Bearing in mind that the Intelligence Services Act, 2000 requires the Directors-General of the intelligence services and the head of the SANAI to take all steps necessary to protect the identities of the members of the services, as well as the methods of intelligence gathering and sources intelligence, the risk of releasing all categories of information should be considered. Even in relation to these categories of information regarded as protected by the Intelligence Services Act, the PAIA, deriving as it does from the constitution, will have greater legal force, and the intelligence services should consider seeking legal advice on aligning these areas with the existing provisions of the PAIA.

An argument favoured by intelligence services the world over, in defence of secrecy, is worth reflecting on. The argument is that little bits of information, disclosed over a period of time, can give away the bigger picture. It is unlikely that a court of law would accept such an argument, since the court would only consider the merits of the information being requested. Thus, the intelligence services should consider whether not releasing certain categories of information on a regular basis, say annual budgets, could not be rendered an incompetent means of protection if counterpoised with the PAIA.

Should the intelligence services feel strongly about the need to effect mandatory protection of certain categories of information, the option of lobbying changes to the PAIA should be

followed. Categories contained in the Intelligence Services Act, as described above could therefore be subject to the provisions of the PAIA. The proper parliamentary procedures would have to be followed, and the intelligence services would have to accept that other interested parties, including freedom of information advocacy groups, would have as much right as they did, in arguing for or against any legislative changes under discussion. An alternative to incorporating as grounds for refusal into the provisions of the Intelligence Services Act that specify which information should be protected by the heads of the services, is to add as a ground for refusal in the PAIA, a category that covers information already protected in terms of existing legislation. The risk in this approach is that there are laws which contradict the spirit of the PAIA, and their integrity may thus be affected.

It has been suggested further, that South Africa requires a law explicitly criminalising espionage. This had been the intention in part of the Protection of Information Act, 1982. However, the provisions of this Act are extremely broad, and critics argue that they place onerous restrictions on members of the civil service and society virtually criminalising the release of vast categories of public records, even where no harm was intended, or has resulted. Moreover, as noted above, many governments in the twenty-first century are considering the need to cooperate with each other, including the sharing of information, and this reality should be taken into account.

An espionage law for South Africa would have to consider carefully, what information of the state, if disclosed to or accessed by a foreign government, would be considered harmful to South Africa's interests, and how such activity would be framed in the criminal law. Taken into account would have to be the increasing range of laws that already deal with specific crimes, proliferation, foreign military assistance, money laundering and corruption, and which are the basis of cooperation between many countries. The more open and accountable to their own people governments are, the less they have to hide from other governments.

It should be remembered that there is no citizenship restriction on who can access information via the PAIA, and wilful governments wanting to access certain information have only to go through the motions in order to access the information. The PAIA already exempts in total certain categories of information, including cabinet records, records of members of

parliament and provincial legislatures, and it is conceivable that the unlawful accessing of these records by agents of a foreign government could constitute a crime of espionage.

Classified records concerning the relationship between the services and their members

The next set of conditions that should be considered is in relation to request for access to records held about themselves that members of the services might seek in terms of the PAIA. One of the aims of the PAIA is to give individuals the opportunity to access records about themselves, so as to correct the records. Intelligence services like all employers, are required to keep personal details about individuals, and should not; generally have reason to withhold information to an individual on these grounds.

More problematic are likely to be those instances where an employee is in dispute with the service and seeks information so as to be able to use it in an internal procedure or in litigation. The Southwood judgment underlined the need for fair and proper administrative procedures on the part of public bodies, but also that the mere fact that a record is classified as confidential, is not grounds to withhold it. Even if it contains third party information, for example testimony about the member by a colleague or any other individual, the service would have to demonstrate whether it considered the severability of the document. The presumption is in favour of disclosure and any body should do all in its efforts to make the document releasable.

The most challenging sub-category in this scenario relates to security clearance investigations. The National Strategic Intelligence Act, 1994 requires the Directors-General to provide procedures for the security screening of individuals who handle classified information. There is a case for records generated in the course of a security screening, to be regarded as operational, whose disclosure could harm the procedure. The timing of the request is the likely issue that would be considered by a court, as would the administrative fairness of the screening procedure. In addition, there is the question of whether the severing of the record had been considered. In South Africa, with its strong rights-based culture, the

courts are likely to consider other rights in such a situation, including the right to work and the right to dignity.

Classified apartheid-era records

Another scenario requiring policy is in relation to requests for access to apartheid-era records, like the TRC files. Apartheid-era records of the state are likely to remain an area of contestation and interest. In several submissions to the CDRC, it was proposed that an urgent audit of such records be undertaken and that they be placed in the custody of the National Archivist. The main concern has been to preserve the integrity of the records, especially in light of the massive destruction of records in the final years of apartheid. The suggestion is laudable, but would require considerable resources. The audit, it is proposed, should consider whether there is any reason for keeping the records out of the public eye and hiving them off to the gloom of the archives. This suggestion is supported, but it is advisable that the role players in the process include not only members of the security and intelligence services, but stakeholders in broader society, such as Parliament, non-governmental organisations and the judiciary. This is in light of the experience of the IRC, whose process was confined to members of the security establishment, resulting in two deficits: one of quality, probably because the breadth of experience in the team was limited, and a resultant deficit of credibility about its findings, which were not made public.

There is merit in the call to put the ghosts of apartheid to rest. There is considerable public unease about claims that are made from time to time, especially about who spied for the apartheid government. A consensus framework for dealing with the secrets of the apartheid era is far preferable to continual and slow leaks about the past. Moreover, disclosure about the methods, and even the objectives, successes and failures of intelligence operations during the apartheid era, could be a considerable salve to those who believe that the truth has been suppressed. This is not to suggest a re-opening of the TRC; its work is done. What is needed is to harness the information released by the process and find a responsible way of releasing it into the public domain.

Currently, the process through which applicants can peruse apartheid files, most commonly about themselves, is the PAIA. The state official, in this case, the archivist, is in a powerful

position in considering such requests, and must decide whether or not the file contains information that must be severed, an alienating procedure. In addition, these records relate only to individuals, and not the policy decisions and directions from political leaders, who were the architects of the system. It is worth government exploring the mass declassification of all such remaining records, and providing the resources for a credible process towards this end.

Classified records about the transition

The transition to democracy marked a significant point in South Africa's political history, and there can be little reason to withhold information about this period from the public. This includes records arising out of the Sub-council on Intelligence under the Transitional Executive Council, and the sub-committees established under the sub-council. These structures were involved in the important work of defining principles and ground rules for the operation of the intelligence services under a future, democratically elected government, while at the same time, trying to steer the existing services towards amalgamation under a democratic government. The South African transition has been held up as a model for the transformation of intelligence services, and a deepened understanding of that process would be a definite result of the bulk declassification and release of documents from that period. The PAIA criteria would have to be applied to determine if there was documentation that could not be released, but by and large these records should be declassified.

Records of oversight authorities investigating the intelligence services

There are a number of oversight institutions who could at any point be required to investigate a matter concerning the intelligence services, and who consequently might be required to access classified information. These bodies include the Inspector-General for Intelligence, the Joint Standing Committee on Intelligence, the South Human Rights Commission, and the Public Protector, among others.

Steytler (2004) argues that when deciding on the most appropriate and effective investigating structure, consideration should be given to a dual investigative approach, e.g. linking an instrument which has access to intelligence information, to a public investigative process. For

example, the Inspector-General for Intelligence, who has full access to the intelligence services, could be used by a Commission of Inquiry or the Human Rights Commission that is closed to those institutions. This will have the effect of inspiring public confidence in the outcome of the inquiry.

It would be incorrect for the scope of an oversight body to be limited by the likelihood that it would come to handle classified information. As stated by Steytler (2004), it would be important for the oversight bodies to be enabled to perform their roles, and this should include granting them access to the classified information, if the area of investigation falls within the parameters of their mandate. Moreover, if the investigating instrument is a credible institution with regard to impartiality and independence, it should be given access to the information necessary to conclude its work, and if necessary take the necessary precautions to protect information from disclosure. Lastly, the investigating instrument has the necessary powers to compel disclosure for both state and private sources.

Concluding remarks

There appear to be no legitimate reasons why the intelligence services should be excluded from aspects of implementing the PAIA, such as the production of a manual. The responsible Executing Authority, the Minister for Intelligence Services should provide the lead on a number of key areas of implementation including the matter of the number of entities. Given the proliferation of structures in the intelligence services, it may be advisable to designate the entire civilian intelligence community under the Ministry for Intelligence Services, as one public body. However, this may prove cumbersome, and the alternative would be for the heads of the two services (NIA and SASS) to provide separate resources for the implementation of the Act.

Whatever is determined, the need for a comprehensive and consistent policy framework is unquestionable. Coordinating this from the level of the Executing Authority is again advisable because it will ensure consistency in dealing with matters pertaining to the operationalising of the Act. The Department of Defence achieved this through a structural arrangement in terms of which the designated Deputy Information Officers came from both the Defence Secretariat and the SANDF.

Another area of implementation that should be reviewed relates to the number of Deputy Information officers. NIA has appointed two (the senior managers responsible for Information Management and Security), whilst SASS was contemplating appointing its Chief Information Officer in this role. Neither structure seems to have contemplated the efficacy of more DIOs. In the case of NIA, the possibility of appointing its heads of the nine provincial offices seems to be an option that could be contemplated. However, this would depend on the degree to which information holdings are decentralised, and the research did not establish the prospects for managing requests for access more efficiently at the local level.

The question of the manuals required in terms of section 14 of the PAIA, will also require attention, because of the intended review in 2008. It is quite possible that the vaguely crafted reasons put forward by the intelligence services for requesting exemption, will not be accepted a second time round. In any case, the services will have been given five years to consider the contents of a manual that can be made publicly available. Under the authority of the Minister, the intelligence services should in fact, look proactively at the question of a manual and aim to place one in the public domain before 2008.

Voluntary disclosure is another area of implementation. Here, the Minister for Intelligence Services has been proactive. All three have websites on which certain corporate information is readily available. But there is a worrying sense in which the provision of this information is discretionary; because its provision is not explicitly projected as being tied to the PAIA, there is a sense in which the largesse of the services could be arbitrarily withdrawn. The Executing Authority for the intelligence services should determine what information the heads of departments will make available publicly, and at what intervals, and publicise these targets so as to be held accountable for their attainment or otherwise. The Joint Standing Committee on Intelligence should also consider a set of minimum standards of disclosure and determine the benefits and pitfalls of casting these in legislation. There is already a solid basis for this since the following oversight authorities require mandatory reports from all public bodies including the intelligence services – as far as possible, they should be free to make their findings public. The Human Rights Commission requires the intelligence services to report on the number of requests dealt with on an annual basis. In terms of the Public Finance Management Act, 1996 (PFMA), the intelligence services are expected to appoint an Audit Committee made up principally of members from outside the services, to advise the

accounting officer on proper financial management of his service. The Auditor-General requires the intelligence services to provide their annual financial statement in terms of prescribed national guidelines, and so as to enable him/her to make a public pronouncement on the state of financial affairs of the intelligence services. And finally, the intelligence services are required to submit information and reports to the JSCI and the Inspector-General, to ensure that these oversight bodies can conduct their functions.

With the exception of the Human Rights Commission, whose interaction with the services is limited to receiving reports about the requests for access to information that have been processed by the services, the other structures mentioned here - the Audit Committee, the Auditor-General, the JSCI and the Inspector-General - all operate within a circle of secrecy, accepting the merits of what the intelligence services have deemed classified. At least in the formative stages of defining - or redefining - what information should be kept secret, it might prove beneficial to the process if these oversight authorities were to be more questioning of why certain information has been designated secret.

Public interest suggests that there is a need for maximum disclosure of surviving records of the apartheid era. The intelligence services should address this need directly, and using the PAIA's benchmark for mandatory protection, disclose all other records of their statutory predecessors that fall into this category. The temptation to interpret the notion of defending national security too broadly should be avoided, as the national security goals of the post-apartheid state are very different to those of the current state.

Several principles might be of use in determining what information from the apartheid past should be protected. Records that reveal the activities and operations conducted by the intelligence services, including their methods, are an important historical resource and may contain important lessons relating to governance and propriety, from which the current intelligence services could gain valuable insight. It is highly unlikely that the operations undertaken in the name of apartheid are still relevant today, and where there are operations that do continue from that period, these should be subject to evaluation by the Executing Authority.

Considerable resources will have to be effected to ensure that records that have already been in the public domain - in particular through the TRC processes - are proactively categorised in strict accordance with the provisions of the PAIA and made accessible. A developing area of contention appears to be those cases where the records are the basis of further legal proceedings, and whether their public disclosure may interfere with the law enforcement process: the DOJ has cited this as one of the main reasons why certain records have been withheld. In a way it is unfortunate that the dispute between the DOJ and SAHA was never considered by the courts; this might have assisted in establishing important maters of principle and precedent. In the absence of such guidance, it might be of use for the Department of Justice to seek independent legal opinion on the matter.

Classified information from the apartheid period should be declassified and archived in a transparent and accessible manner, possibly along the lines which the Defence Archives is managed. A periodisation of the records from the time of the formation of the Bureau for State Security (BOSS) could be considered; this would be of great value to historians and could contribute to the growth of scholarship in this field.

The records from the period of transition, particularly from the TEC period, should be universally declassified and made available through the Department of Justice, where they are all currently housed. Again, this was a period rich in debate and content, a considerable amount of which happened behind closed doors. Students and society could benefit in their understanding about the role of intelligence services in this period, as well as learn about the creation of the new intelligence services, through a study of the declassified records.

For the post 1994 period, apart from implementing those aspects of the PAIA which have been discussed above, the intelligence services should carefully assess how the exceptions affect the information currently in their possession and information they routinely generate or come into possession of. It would also be useful for the intelligence services to study judgements in relation to confidential information, as in the case of CCII Systems (Pty) Ltd v the Minister of Defence (Southwood), as these precedents could have a bearing on the acceptability of grounds for refusal to disclose information in future.

Given the complexity of the issues, strong leadership and policy direction will be needed. The Minister responsible should ensure that the issues, including the historical and constitutional imperatives, are clearly understood within the intelligence services, determine policy objectives for the intelligence services and a programme of action in motion. On the other hand, there is a need for vigilance on the part of society, the courts and oversight bodies. The intelligence services should be challenged and held to account, yet should also be given the opportunity and platforms to explain their challenges so that society can make input on how to balance the imperatives.

Lastly, adequate resources including trained and service-oriented personnel, improved information management systems, and the physical infrastructure to make voluntary disclosure as well as responses to disclosure a reality. Consideration should be given to relating to people in all the official languages of the country, and to educating the public about the role and duties of the intelligence services through accessible media.

INTERVIEWS *

Ackermann, Marius (Advocate), former Law Advisor to the Office of the State President 1987-1994, 28 August 2003

Cwele, Siyabonga (Dr), Chairperson, Joint Standing Committee for Intelligence, 11 August 2005

Dennis, Hilton (Mr), Director-General, South African Secret Service, 25 July 2005

Dlomo, Dennis (Mr), Head Ministerial Services, Ministry for Intelligence Services, 26 August 2003

Dominy, Graham (Dr), National Archivist, Department of Arts, Culture Science and Technology, 2 September 2003

Geldenhuys, Tertius (Dr), Head Legal Services, South African Police Service, 7 October 2003

Harris, Verne (Mr), Director, South African History Archive, 1 September 2003

Hendricks, Wayne (Dr), Senior Analyst in the National Intelligence Coordinating Committee (NICOC), and former head of Access to Information Unit, Department of Defence, 28 July 2005

Masetlha, Billy (Mr), Director-General, National Intelligence Agency, 4 August 2005

McKay, Jackie (Mr), Deputy Information Officer, National Intelligence Agency, 15 July 2005

Netshitenzhe, Takalani (Ms), Head: Legal and Constitutional Services, Ministry for Intelligence Services, 26 August 2003

Ngcakani, Zolile (Mr), Inspector-General of Intelligence, 3 August 2005

Porogo, David (Mr), Deputy Information Officer of the Department of Justice and Constitutional Development, 27 August 2003

Raswiswi, Marlyn (Ms) Deputy Information Officer, Department of Justice and Constitutional Development, 4 August 2005

Shaik, Moe (Mr), Head: Policy Unit in the Department of Foreign Affairs, RSA and former Deputy Coordinator, NICOC, 17 October 2003

Van Heerden, Wallie (Mr), Executive Manager, Office of the Auditor-General, 21 October 2003

Van Schoor, Empie (Ms), Director: Legal Services in Department of Public Service and Administration. Former State Law Advisor and member of the Task Team appointed by the President to draft the Open Democracy Bill, 25 August 2003

Wessels, Leon (Dr) Commissioner of the Human Rights Commission, South Africa, 2 August 2005

** Unless otherwise indicated, positions reflected are those held by interviewees at the time that interviews were conducted.*

REFERENCES

LEGISLATION

South Africa

Republic of South Africa. 1978. Bureau for State Security Act, No. 104, 1978. Pretoria: Government Printer.

Republic of South Africa. 1972. Security Intelligence and State Security Council Act, No.64, 1972. Pretoria: Government Printer.

Republic of South Africa. 1982. Protection of Information Act, No. 84, 1982. Pretoria: Government Printer.

Republic of South Africa. 1993. Transitional Executive Council Act, 1993.

Republic of South Africa. 1993. Constitution of the Republic of South Africa, No. 200 of 1993. Pretoria: Government Printer.

Republic of South Africa. 1994. Intelligence Services Control Act, No.40, 1994. Pretoria: Government Printer.

Republic of South Africa. 1995. Promotion of National Unity and Reconciliation Act, No. 34, 1995. Pretoria: Government Printer.

Republic of South Africa. 1996. National Archives Act, No. 43, 1996. Pretoria: Government Printer.

Republic of South Africa. 1996. The Constitution of the Republic of South Africa, No 108, 1996. Pretoria: Government Printer.

Republic of South Africa. 1999. Public Finance Management Act, 1999. Pretoria: Government Printer.

Republic of South Africa. 2000. Promotion of Access to Information Act, No.2, 2000. Pretoria: Government Printer.

Republic of South Africa. 2002. Intelligence Services Act, 2002. Pretoria: Government Printer.

Republic of South Africa. 2002. Electronic Communications and Transactions Act, No. 25 of 2002. Pretoria: Government Printer.

Republic of South Africa. 2002. Regulation of Interception of Communications and Provision of Communications Related Information Act, No. 70 of 2000. Pretoria: Government Printer.

United States of America

United States of America. 1966. Freedom of Information Act.

United States of America. 1976. Government in the Sunshine Act.

United States of America. 1976. Privacy Act.

United States of America. 1980. Classified Information Procedures Act.

United States of America. Executive Order 12356, 2 April 1982

Canada

Canada. 1982. Access to Information Act.

Canada. 1982. Privacy Act.

India

India. Right of Information Bill, 2004. http://www.privacyinternational.org (2005/08/29).

The Rajasthan Right to Information Act, 2000 (Act. 13 of 2000). http://www.rajgovt.org/right_to_info/act2000

OFFICIAL DOCUMENTS

South Africa

Department of Defence. 2000. *Department of Defence Instruction: Pol&Plan/00034/2000. Policy on the Implementation of the Promotion of Access to Information Act.*

Department of Defence. 2003. *Access to Information manual.* Pretoria.

South Africa. 1981. *Report of the Rabie Commission of Inquiry into Security Legislation*. Pretoria: Government Printer.

South Africa. *Minimum Information Security Standards*. Approved by Cabinet 4 December 1996.

South Africa. 1995. *White Paper on Intelligence*. Pretoria: Government Printer.

South Africa. 1998. *Truth and Reconciliation Commission, Volume 1. Chapter 8* (http://www.doj.gov.za/trc/report).

National Intelligence Service, 1994. *Twenty Fifth Anniversary brochure.*

Task Group on Open Democracy. *Open Democracy Act for South Africa. Policy Proposals.* 19 January 1995.

Annual Report of the Joint Standing Committee on Intelligence, 1997.

Report of the Auditor-General, 1996/1997.

Report of the Auditor-General, 1997/1998

South Africa. Hansard, 12 May 1996.

United States

United States of America. 1997. *Report of the Commission on Protecting and Reducing Government Secrecy. USA* Government Printing Office. Washington.

Canada

Canada. 2001. *Report of the Access to Information Review Task Force.* http:/www.atirtf - geai.gc.ca/paper-scope_atia-e.html (10/18/02).

COURT PAPERS AND JUDGMENTS

Founding affidavit by Sello Hatang in the High Court of South Africa (Transvaal Provincial Division), in the matter of South African History Archive Trust versus the Minister of Justice and Constitutional Development, and David Porogo (25 November 2002).

Affidavit by David Porogo, in High Court of South Africa (Transvaal Provincial Division) in the matter of South African History Archive Trust versus The Minister of Justice and Constitutional Development, and David Porogo (22 December 2003).

Replying Affidavit by Sello Hatang in the High Court of South Africa (Transvaal Provincial Division), in the matter of South African History Archive Trust versus The Minister of Justice and Constitutional Development, and David Porogo (22 January 2004).

Supplementary Affidavit by Sello Hatang in the High Court of South Africa (Transvaal Provincial Division) in the matter of South African History Archive Trust versus The Minister of Justice and Constitutional Development, and David Porogo (22 January 2004).

Supplementary Affidavit by David Porogo in the High Court of South Africa (Transvaal Provincial Division), in the matter of South African History Archive Trust versus The Minister of Justice and Constitutional Development, and David Porogo (12 February 2004).

Affidavit of Reply to Respondent's Supplementary Affidavit by Sello Hatang in the High Court of South Africa (Transvaal Provincial Division) in the matter of the South African Archive Trust versus The Minister of Justice and Constitutional Development, and David Porogo (25 February 2004).

Judgement of Justice Southwood in the matter between CCII Systems (Pty) Limited and MPG Lekota, in the High Court of South Africa (Transvaal Provincial Division), 2002.

BOOKS, JOURNAL ARTICLES, UNPUBLISHED PAPERS, INTERNET AND NEWSPAPER ARTICLES

Ackroyd, S. and Hughes, J. 1992. *Data collection in context (2nd edition).* London: Longman.

Adler, A.R. 1991. *Litigation under the federal open government laws*. Washington: ACLU.

Africa, S. 1994. Removing the shroud of secrecy, in MPD News Vol. 3 No. 3 September (Newsletter of the Institute for Multiparty Democracy).

Africa, S. & Mlombile, S. 2001. *The transformation of the South African intelligence services.* Paper presented to Round Table on the Reform of the Guatemalan Intelligence Service, hosted by Project on Justice in Times of Transition. Harvard University, Boston..

Africa, S. (1992). The SABTVC intelligence services during an interim government period, in Strategic Review for Southern Africa, Vol. XIV no. 2 October 1992. Institute for Strategic Studies, University of Pretoria

African National Congress. (1992) *ANC policy guidelines for a democratic South Africa.* As adopted at ANC national conference 28-31 May 1992, Durban.

Aguero, F. (2005). *The new 'double challenge': simultaneously crafting democratic control and efficacy concerning military, police and intelligence.* Geneva Centre for the Democratic Control of Armed Forces – Working paper No. 161.

Al-Mashat, A. (1985). *National security in the Third World*. London: Westview Press.

Aubrey, C. (1981). *Who's watching you? Britain's security services and the Official Secrets* Act. Harmondsworth: Penguin Books.

Azar, E. & Moon, C. (eds). (1988). *National security in the Third World. The management of internal and external threats*. Hants: Edward Elgar Publishing Limited.

Banisar, S. 2002. *Freedom of information and access to government records around the world.* Privacy International.

Beaufre, A. 1965. *An introduction to strategy, with particular reference to problems of defence, politics, economics, and diplomacy in the nuclear age.* London: Faber and Faber.

Bell, T. 2001. *Unfinished business. South African apartheid and truth.* Cape Town: Red Works.

Bindman, G (ed). 1988. *South Africa. Human rights and the rule of law.* London, New York: Pinter Publishers.

Blackbeard, M. HIV/AIDS: the right to privacy vs the right to life in Journal of Contemporary Roman Dutch Law, Vol. 65, no. 2, May 2002, pp. 232-241.

Blackburn, D. & Cadell, W. 1911. *Secret service in South Africa*. London, New York, Toronto and Melbourne: Cassell and Company, Ltd.

Bok, S. 1978. *Lying - moral choice in public and private life*. New York: Pantheon Books.

Bok, S. 1982. *Secrets - on the ethics of concealment and revelations*. New York: Pantheon Books.

Bond, P. 2000. *Elite transition: from apartheid to neo-liberalism in South Africa.* London; Sterling, Va.: Pluto Press.

Booth, K. (ed). 1991. *New thinking about strategy and international security.* London: Harper Collins.

Born, H (ed). 2003. *Parliamentary oversight of the Security Sector. Principles, mechanisms and practices.* Geneva: IPU& CDAF.

Breytenbach, W. Security and intelligence structures: regionalism and the federal/unitary debate, in Strategic Review for Southern Africa, Vol. XIV, no. 2 October 1992. Institute for Strategic Studies, University of Pretoria.

Brodeur, J., Gill, P. & Tollberg, D. 2003. *Democracy, law and security. Internal security services in contemporary Europe*. Hampshire: Ashgate Publishing Limited.

Brogden, M. & Shearing, C. 1993. *Policing for a New South Africa.* London, New York: Routledge.

Burns, Y. Freedom of expression under the new Constitution. in Comparative and International Law Journal of South Africa, Vol. 30, no. 3, November 1997, pp. 264-286.

Bursey, G.J. Privilege and police dockets, in The Magistrate, Vol. 25, No. 4, December 1990, pp. 122-140.

Buzan, B. Rethinking security after the Cold War, in Nordic Journal of International Studies, Vol. 32 No. 1. March 1997, pp. 5 - 28.

Buzan, B. People states and fear: the national security problem in the Third World, in Azar, E. & Moon, C. (eds). 1988. *National security in the Third World. The management of internal and external threats*. Hants: Edward Elgar Publishing Limited.

Buzan, B., Waever, O. & de Wilde, J. 1998. *Security: a new framework for analysis.* Boulder, London: Lynne Rienner Publishers.

Carnelley, M. Recent case law: confidentiality and the right of access to information in the application procedures for casino licences, in De Jure, Vol. 32, no. 2, 1999, pp. 330 -339.

Cassim, F. Police docket privilege, in Codicillus, Vol. 37, no. 1, May 1996, pp. 113 -115.

Cawthra, G. 1986. *Brutal force. The apartheid war machine.* London: International Defence and Aid Fund for Southern Africa.

Cawthra, G. & Luckham, R. 2003. *Governing insecurity – democratic control of military and security establishments in transitional democracies.* London, New York: Zed Books.

Cherry, J., Daniel, J. & Fullard, M. Researching the ' Truth': A view from inside the Truth and Reconciliation Commission, in Posel, D and Simpson, G. 2002. *Commissioning the past. Understanding South Africa's Truth and Reconciliation Commission.* Johannesburg: Witwatersrand University Press.

Childs, D. & Popplewell, R. 1996. *The Stasi - the East German intelligence and security service.* London: MacMillan Press Ltd.

Chuter, D. 2000. *Defence transformation – a short guide to the issues.* Pretoria: Institute for Security Studies.

Cilliers, J. 2003. *Peace and security through good governance: a guide to the NEPAD African Peer Review Mechanism.* Pretoria: Institute for Security Studies.

Cilliers, J. 2005. *Towards a continental early warning system for Africa.* Pretoria: Institute for Security Studies.

Cock, J. & Nathan, L.(eds) 1989. *War and society: the militarization of South Africa.* Cape Town: David Philip; New York: St Martin's Press.

Cohen, R.N. 1982. *Whose file is it anyway?* London: National Council for Civil Liberties.

Coliver, S., Hoffman, P.Fitzpatrick, J & Bowan, S. (ed) 1999. *Secrecy and liberty: national security, freedom of expression and access to information.* The Hague/Boston/London: Martinus Hijhoff Publishers.

Collinge, J. Launched on a bloody tide - negotiating the new South Africa, in Moss, G & Obery, I. (eds) South African Review. From 'Red Friday' to CODESA. Braamfontein: Ravan Press.

Currie, I. Substantive provisions of the Bill of Rights, in Annual survey of South African Law, 1999, pp. 50-71.

Currie, I. 2000 Bill of rights jurisprudence, in Annual survey of South African Law, 2000, pp. 24 - 38.

Currie, I. & Klaaren, J. (2002). *The Promotion of Access to Information Act commentary*. Cape Town: Siber Ink.

D'Souza, F. Foreword. in Coliver, S., Hoffman, P.Fitzpatrick, J & Bowan, S. (ed) 1999. *Secrecy and liberty: national security, freedom of expression and access to information.* The Hague/Boston/London: Martinus Hijhoff Publishers.

Davidson, B., Slovo, J. & Wilkinson, A. 1976. *Southern Africa. The new politics of revolution.* Harmondsworth: Penguin Books.

De Coning, C. The nature and role of public policy, in Cloete, F. & Wissink, H. (ed) 2000. *Improving public policy.* Pretoria: Van Schaik Publishers.

De Kiewiet, C. W. 1941. *A history of South Africa - social and economic.* London: Oxford University Press.

De Villiers, W. The interim bill of fundamental human rights: a prosecutor's perspective, in Journal of Contemporary Roman-Dutch Law, No 1, 1995, pp. 133-140.

De Villiers, W. An appraisal of the right of access to information held by police or state officials for purposes of a bail application under Canadian and South African law (part 1), in Journal of Contemporary Roman-Dutch Law, Vol. 66, no. 2, May 2003, pp.175-184.

De Vos, W. The impact of the new Constitution upon civil procedural law, in Stellenbosch Law Review, Vol. 6, no. 1, 1995, pp. 34-53.

Deale, P. Opening the books, in Employment Law, Vol. 10, no. 6, July 1994, pp. 130-131.

De Coning, C. The nature and role of public policy, in Cloete, F. &Wissink, H. (eds.) 2000. *Improving public policy.* Pretoria: Van Schaik Publishers.

Dlomo, D. *Intelligence in Practice: South Africa's legislative transformation of 2002.* (unpublished paper, 2004).

Dorn, A.W. 1999. The cloak and the blue beret: the limits of intelligence-gathering in UN peace-keeping, in The Pearson Papers (No.4 – Intelligence in Peacekeeping), Canadian Peacekeeping Press.

Driver-Jowet, J.P. Access to medical information, in De Rebus, No. 365, June 1998, p. 25.

Du Plessis, W. The right to environmental information in the new national Environmental Management Bill, in South African Journal of Environmental Law and Policy, Vol. 5, no. 2, November 1998, pp. 395 – 403.

Du Plessis, W. Enforcement of environmental rights by way of a right to information, in Obiter, Vol. 20, no. 1, 1999, pp.92 – 112.

Dunn, W.N. 1994. (ed) *Public Policy Analysis: An Introduction (Second Edition).* New Jersey: Prentice Hall.

Evatt, E. The International Covenant on Civil and Political Rights: freedom of expression and state security, in Coliver, S., Hoffman, P. Fitzpatrick, J & Bowan, S. (ed) 1999. *Secrecy and liberty: national security, freedom of expression and access to information.* The Hague/ Boston/ London: Martinus Hijhoff Publishers.

Federation of American Scientists (FAS) Intelligence Resource Programme. *Laws and Regulations –Indian Intelligence Agencies* (http://www.fas.org/irp/ 11/09/2001).

Franck, T and Weisband, E. (eds). 1972. *Secrecy and foreign policy.* London: Oxford University Press.

Freedman, L. Whither nuclear strategy, in Booth, K. (ed). 1991. *New thinking about strategy and international security.* London: Harper Collins.

Friedman, S. 1993. *The long journey. South Africa's quest for a negotiated settlement.* Johannesburg: Ravan Press.

Galtung, J. 1984. *There are alternatives! Four roads to peace and security.* Nottingham: Spokesman.

Garnett, J. (ed). 1970. *Theories of peace and security. A reader in contemporary strategic thought.* London: Macmillan.

Gaum, L. The right of access to information. *Case name: Corf v Health Professions Council of South Africa 2000 (1) SA 1171(T)*, in Journal of Contemporary Roman-Dutch Law , Vol. 64, no. 1, February 2001, pp. 146 -155.

Geldenhuys, D. 1984. *The diplomacy of isolation: South African foreign policy making.* Johannesburg: McMillan.

Gerhardt, G.M. 1978. *Black power in South Africa. The evolution of an ideology.* Berkeley, Los Angeles, London: University of California Press.

Gilliomee, H. & Schlemmer, L. 1989. *From apartheid to nation-building.* Cape Town: Oxford University Press.

Glazewski, J. The environment and the new interim constitution, in South African Journal of Environmental Law and Policy, Vol. 1, no. 1, March 1994, pp. 3 -16.

Govender, K. Access to Information: enforcement mechanisms and fees, in SA Public Law, Vol. 10, No. 2, 1995, pp. 346-355.

Grinlinton, D. Access to environmental justice in New Zealand, in Acta Juridica, 1999.

Grogan, J. Equal justice: union access to executive hearings, in Employment Law, Vol. 13, No. 4, June 1997, pp. 79 -80; 92.

Grundy, K. 1987. *The militarization of South African politics.* Oxford: Oxford University Press.

Guy, R., Edgley, C., Arafat, I. & Allen, D. 1987. *Social research methods. Puzzles and solutions.* Boston, London, Sydney, Toronto: Allen & Bacon, Inc.

Halperin, M. & Hoffman, D. 1977. *Top secret: national security and the right to know.* New Republic Books: Washington.

Hamilton, C., Harris, V., Taylor, J., Pickover, M, Reid, G. & Saleh, R. 2002. *Refiguring the Archive.* Cape Town: David Philip.

Hansson, D. *Changes in counter-revolutionary state strategy in the decade 1979 to 1989* in Hansson, D. and van Zyl Smit, D. (eds). 1990. *Towards justice? Crime and state control in South Africa.* Cape Town: Oxford University Press.

Harris, V. *Where are the TRC records*? in Natal Witness, 22 April 2002.

Harris, V. *They should have destroyed more: the destruction of official memory under apartheid* in Transformation, (2) 2000.

Harris, V. *Using the Promotion of Access to Information Act (PAIA): The case of the South African History Archive.* Unpublished paper.

Hauerwas, S. & Lentricchia, F. 2003. *Dissent from the homeland. Essays after September 11.* Durham, London: Duke University Press.

Hayner P., 2001. *Unspeakable truths. Confronting state terror and atrocity.* New York, London: Routledge.

Haysom, N. 1992. Negotiating a political settlement in South Africa, in Moss, G. & Obery, I. 1992. *South African Review 6. From 'Red Friday' to CODESA*. Braamfontein: Ravan Press.

Hazell, R. Freedom of information in Australia, Canada and New Zealand, in Public Administration, Vol. 67 Summer 1989 (189-210).

Henderson, R. South African Intelligence transition from de Klerk to Mandela: An Update, in Journal of Intelligence and Counterintelligence, Vol. 8. no. 6, pp. 471- 485.

Hodess, R. (ed). 2003. *Transparency International Global corruption report. Special focus: access to information.* London: Profile Books.

Hough, M. The SABTVC and liberation movements' intelligence services in a changing SA, in Strategic Review for Southern Africa, Vol. XIV No. 2 October 1992. Institute for Strategic Studies, University of Pretoria.

India Together. *The Freedom of Information Bill 2000.* (http://www.indiatogether.org/rti/, 23 January 2006).

ISSUP (Institute for Strategic Studies University of Pretoria). 1992. *Selected Official South African Strategic Perceptions 1989 -1992.* University of Pretoria.

Jazbhay, S.A. Recent constitutional cases, in De Rebus No. 351, April 1997, pp. 254-256.

Jazbhay, S.A. Recent constitutional cases, in De Rebus, No. 413, July 2002, pp. 45-47.

Jazbhay, S.A. Recent constitutional cases, in De Rebus No. 362, March 1998, pp. 41 -43.

Jones, R. Message in a bottle: theory and praxis in Critical Security Studies, in Contemporary Security Policy, Vol. 16 No. 3, December 1995. London: Frank Cass.

Kaldor, M. Rethinking Cold War history in, Booth, K. (ed). 1991. *New thinking about strategy and international security*, London: Harper Collins.

Kaldor, M. (ed). 2000. *Global insecurity.* London, New York: Pinter.

Kidd, M. The National Environmental Management Act and public participation, in South African Journal of Environmental Law and Policy, Vol. 6, no. 1, May 1999, pp. 21-31.

Klaaren, J. 2002. *The Gap Report. Issues regarding the disclosure of information by public officials.* Paper produced for South African History Archive.

Lala, A. Picturing the landscape: police, justice, penal and intelligence reforms in Africa, in Ferguson, C. & Isima, J. O. (eds). 2004. *Providing security for people: enhancing security through police, justice, and intelligence reform in Africa.* Shrivenham: Global Facilitation Network for Security Sector Reform.

Landman, A.A. Labour's right to employer information, in Contemporary Labour Law, Vol. 6, no. 3, October 1996, pp. 21-25.

Lansford, T. 2002. *All for one. Terrorism, NATO and the United States.* Hampshire: Ashgate Publishing Limited.

Le Roux, L., Rupiya, M. & Ngoma, N. (eds.) 2004. *Guarding the guardians. Parliamentary oversight and civil-military relations: the challenges for SADC.* Pretoria: Institute for Security Studies.

Le Roux, P.A. K. Access to information: the Promotion of Access to Information Act and implications for employers, in Contemporary Labour Law, Vol. 10, no.11, June 2001, pp.101-110.

Lee, R. Making public policy: heart of the political process, in Cloete, F. Schlemmer, F. van Vuuren, D. (eds) 1991. *Policy options for a new South Africa.* Pretoria: HSRC Publishers.

Lee, R. and Schlemmer, L. 1991 *Peace and security. The next generation.* Lanham, Maryland: Rowman and Littlefield.

Leigh, I. 1997. Legal access to security files. The Canadian experience, in Intelligence and National Security, Vol.12, no. 2 (pp. 126-153)

Levy, N. (Ed) 2004. *Balancing secrecy and transparency in a democracy. Hefer Commission - the case study*. South African National Academy of Intelligence.

Lipinski, T. 1999. *Globalisation of Information and the Post National Era: Critical choices for the new millenium and beyond. The moral and legal challenges of the information era* Unpublished conference paper. Pretoria.

Lopez, G. & Myers, N.J. 1998. *Peace and security. The next generation.* Lanham, Maryland: Rowman and Littlefield.

Lustgarten, L. and Leigh, I. 1994. *In from the cold: national security and parliamentary democracy.* Oxford: Clarendon Press.

Magubane, B. (ed). 2004. *The Road to Democracy in South Africa. Volume 1 (1960 - 1970).* Cape Town: Zebra Press.

Malan, F.R. Oor inligting, rekenaarmisbruik en die strafreg, in De Jure, Vol. 22, No. 2, 1989, pp. 211-232.

Malan, M. & Cilliers, J. *SADC Organ on Politics, Defence and Security: Future development.* Institute for Security Studies Occasional Paper No. 19, March 1997

Martin, R. & Feldman, E. 1998 *Working Paper: Access to information in developing countries.* Transparency International (www.transparency.org/working_papers dated 1/13/03).

Mates, M. 1989. *The secret services: is there a case for greater openness?* London: Allied Publishers.

Mathews, A. S. 1971. *Law, order and liberty in South Africa.* Cape Town, Wetton, Johannesburg: Juta and Company, Ltd.

Mathews, A. S. 1978. *The darker reaches of government. Access to information about public administration in three societies.* Cape Town: Juta and Company Limited.

Matlala, D. *Law reports: access to information. Case name: Ingledew v Financial Services Board 2003 (4) SA 584(CC)* in De Rebus, No. 427, October 2003, p.41.

Modise, T. 2004. Parliamentary oversight of the South African Department of Defence, in Le Roux, Rupiya &Ngoma (eds.) 2004. *Guarding the guardians. Parliamentary oversight and civil-military relations: the challenges for SADC.* Pretoria: Institute for Security Studies.

McGoldrick, D. 2004. *From 9/11 to the Iraq War 2003: international law in an age of complexity.* Oxford, Portland, Or: Hart Publishers.

McKinley, D. T. 2004. *The state of access to information in South Africa.* Research report written for the Centre for the Study of Violence and Reconciliation, Johannesburg.

McLaurin, R.D. Managing national security: the American experience and lessons for the Third World, in Azar, E. & Moon, C (eds). (1988). *National security in the Third World. The management of internal and external threats*. Hants: Edward Elgar Publishing Limited.

Meintjies-Van der Walt, L. Pre-trial disclosure in criminal cases: the implications of section 23 of the Interim Constitution in SAC, Vol. 8, no. 2, 1995, pp. 127-141

Moss, G, & Obery, I. (eds). 1992. *South African Review: From "Red Friday to CODESA.* Johannesburg: Ravan Press.

Mureinik, E. A bridge to where? Introducing the interim bill of rights, in South African Journal of Human Rights, Vol. 10. no. 1, 1994, pp. 31- 48

Nathan, L. Good governance, security and disarmament in Africa, in African Journal of Political Science (1998), Vol. 3, no. 2, pp. 69-79

Nathan, L. *Towards a conference on security, stability, development and cooperation in Africa.* Unpublished paper presented at the Asian Peace Research Conference, New Zealand. January-February 1992.

Nathan, L. & Phillips, M. 'Cross currents'. Security developments under FW de Klerk, in Moss, G. & Obery, I. (eds.)1992. *South African Review: From "Red Friday to CODESA.* Johannesburg: Ravan Press.

Netshitenzhe, T. 2005. *A comparative analysis of the roles and functions of the Inspector-General of Intelligence with specific reference to South Africa.* Unpublished MA dissertation, University of Pretoria.

Nhlanhla, 1992.The SABTVC and liberation movements. Modalities of combining their intelligence services, in Strategic Review for Southern Africa, Vol. XIV, No. 2. October 1992.

Nicol, A. *The European Union: National security restrictions, human rights and information in the public interest,* in Coliver, S., Hoffman, P.Fitzpatrick, J & Bowan, S. (ed) 1999. S*ecrecy and liberty: national security, freedom of expression and access to information*. The Hague/Boston/London: Martinus Hijhoff Publishers.

O'Brien, K. South Africa's evolving intelligence and security structures, in International Journal of Intelligence and Counterintelligence, 9:2 (Summer 1996):187-232.

Oyebade, A. and Alao, A. (eds). 1998. *Africa after the Cold War. The changing perspectives on security.* Asmara: African World Press.

Paraschos, E. 1975. *National Security and the People's Right to know.* Unpublished dissertation submitted to the Faculty of the Graduate School, University Missouri-Columbia in partial fulfilment of the requirements for the degree Doctor of Philosophy.

Parsons, W. 1995. *Public policy. An introduction to the theory and practice of policy analysis.*

Petersen, B. The archives and the political imaginary, in Hamilton, C., Harris, V., Taylor, J., Pickover, M, Reid, G. & Saleh, R. 2002. *Refiguring the archive*. Cape Town: David Philip.

Pigou, P. False promises and wasted opportunities: inside South Africa's Truth and Reconciliation Commission, in Posel, D. and Simpson, G. G. 2002. *Commissioning the past. Understanding South Africa's Truth and Reconciliation Commission.* Johannesburg: Witwatersrand University Press.

Pimstone, G. Going quietly about their business: access to corporate information and the Open Democracy Bill, in South African Journal of Human Rights, Vol. 15, no. 1, 1999, pp. 2- 4.

Posel, D. & Simpson, G. 2002. *Commissioning the past. Understanding South Africa's Truth and Reconciliation Commission.* Johannesburg: Witwatersrand University Press.

Pottinger, B. Sunday profile: *The low-down on SA's new spymaster,* in Sunday Times, 23 February, 1992.

Qunta, C. The tension between secrecy and transparency in a democracy: the legal process and intelligence constraints in Levy, N. 2004. (ed) 2004. *Balancing secrecy and transparency in a democracy. Hefer Commission - the case study*. South African National Academy of Intelligence.

Rankin, M. National security: information, accountability and the Canadian Security Intelligence Service, in University of Toronto Law Journal (1986), Vol. 36. (249-286).

Rauch, J. 1991. *The challenges for policing in the new South Africa: policing the violence,* Paper presented to the American Society of Criminologists Conference, San Fransisco.

Ray, E. 1979. *Dirty Work 2: the CIA in Africa.* Secaucus: N.J.: Lyle Stuart.

Rhoodie, E. 1983. *The Real information scandal.* Pretoria: Orbis (SA) Pty Ltd.

Richelson, J. T. 1989. *The U.S. intelligence community (Second edition)*. USA: Harper Business.

Robertson, KG. 1999. *Secrecy and open government.* London: MacMillan Press Ltd.

Roos, A. Data protection provisions in the Open Democracy Bill, 1997, in Journal of Contemporary Roman Dutch Law, Vol. 61, no.3, August 1998, pp. 497-506.

Rupiya, M. 2004. An African perspective of the reform of the security sector since the 1990s, in Le Roux, Rupiya &Ngoma (eds.), Le Roux, L., Rupiya, M. & Ngoma, N. (eds.) 2004.

Guarding the guardians. Parliamentary oversight and civil-military relations: the challenges for SADC. Pretoria: Institute for Security Studies.

SAFM, *Interview with National Archivist, Dr Graham Dominy, November 2003.*

Schneier, B. 2003. Beyond Fear: Thinking Sensibly about Security in an Uncertain World. New York: Copernicus Books.

Schulze, H. *The law reports: Company law* in De Rebus, No. 431, March 2004, p. 34.

Scraton, P. (ed) 2002. *Beyond September 11: an anthology of dissent.* London: Pluto Press.

Seegers, A. 1996. *The military in the making of modern South Africa.* London: Tauris.

Shaw, M. *Spying for democracy. Intelligence, the new world order and South Africa.* Paper presented to Policy Seminar: The security forces and the Constitution. Caper Town, 15 February 1995.

Shulsky, A. 1991. *Silent Warfare: understanding the world of intelligence.* Brassey's (US) Inc.

Simpson, G. 'Tell no lies, claim no easy victories': A brief evaluation of South Africa's Truth and Reconciliation Commission, in Posel, D. & Simpson, G. 2002. *Commissioning the Past. Understanding South Africa's Truth and Reconciliation Commission.* Johannesburg: Witwatersrand University Press.

Smith, A, 1983. *State and nation in the Third World. The western state and African nationalism.* Brighton: Wheatsheaf Books.

Solomon, P. Law of taxation: the interim constitution: 1995 survey: section 23 of the interim constitution, in Annual Survey of South African Law, 1995, pp. 690 - 692.

Southall, R. Restructuring intelligence for post-apartheid South Africa, in Strategic Review for Southern Africa, Vol. XIV No. 2, October 1992, Institute for Strategic Studies, University of Pretoria

Steele, P. 2001. *On intelligence. Spies and secrecy in an open world.* Oakton, Virginia: OSS International Press.

Steytler, N. A legal framework for investigations affecting the intelligence services, in Levy, N. (ed) 2004. *Balancing secrecy and transparency in a democracy. Hefer Commission - the case study*. South African National Academy of Intelligence.

Strauss, S.A. Legal issues concerning AIDS, an outline, in SAPM, Vol. 9, No. 1, 1998, pp.13-14.

Subrahmanyan, K. 2000 *Challenges to Indian security* (http://www.idsa-india.org/an-dec-00-1.html).

Swilling, M. & Phillips, M. The powers of the thunderbird. Decision-making structures and policy strategies in the South African state, in Centre for Policy Studies, University of the Witwatersrand (eds). 1989. *South Africa at the end of the eighties. Policy perspectives 1989.* Johannesburg: Centre for Policy Studies.

Taylor, I. & Vale, P. South Africa's transition revisited: globalisation as vision and virtue, in Global Society, Vol. 14, No. 3, 2000.

Terreblanche, C. & Bell, T. *Maduna allows the NIA to slip under a blanket of secrecy,* in Sunday Independent, 25 May 2003.

Thomas, C. New directions in thinking about security in the Third World, in Booth, K. (ed). 1991. *New Thinking about Strategy and International Security*. London: Harper Collins.

Todd, P. & Bloch, J. 2003. *Global intelligence. The world's secret services today.* London, New York: Zed Books.

Turner, S. 1986. *Secrecy and democracy. The CIA in transition.* London: Sidgwick.

Van der Poel, J. Omissions and a doctor's legal duty to warn identifiable sexual partners of HIV positive patients, in Responsa Meridiana, 1998, pp. 18 – 40.

Van Diepen, M.(ed). 1988. *The national question in South Africa*. London, New Jersey: Zed Books Ltd.

Van Niekerk, L. E. 1985. *Kruger se regterhand. A biografie van Dr W. J. Leyds.* Pretoria: J.L. van Schaik.

Van Oosten, F. The law and ethic of information and consent in medical research, in Journal of Contemporary Roman-Dutch Law, Vol. 63, no. 1, February 2000, pp. 5 – 31.

Van Wyk, C. W. HIV of Vigs op doodsertifikate, in Journal of Contemporary Roman-Dutch Law ,Vol. 59, no. 4, November 1996, pp. 626 – 635.

Visser, P.J. Some principles regarding the requester of access to a record and related issues in terms of the Promotion of Access to Information Act 2 of 2000, in Journal of Contemporary Roman-Dutch Law, Vol. 65, no. 2, May 2002, pp. 254 - 256.

Wessels, J. Legislative drafting and legislation giving effect to the Constitution, in SA Public Law, Vol. 17. No. 1, 2002, pp. 131 – 141.

Williams, K. and Deletant, D. 2001. *Security intelligence services in new democracies. The Czech Republic, Slovakia and Romania.* Hampshire, New York: Palgrave.

Yin, R.K. 2003. *Applications of case study research (Second edition).* Sage Publications.

Zulu, P. The Hefer Commission: a comparative perspective, in Levy, N. (ed) 2004. *Balancing secrecy and transparency in a democracy. Hefer Commission - the case study*. South African National Academy of Intelligence.