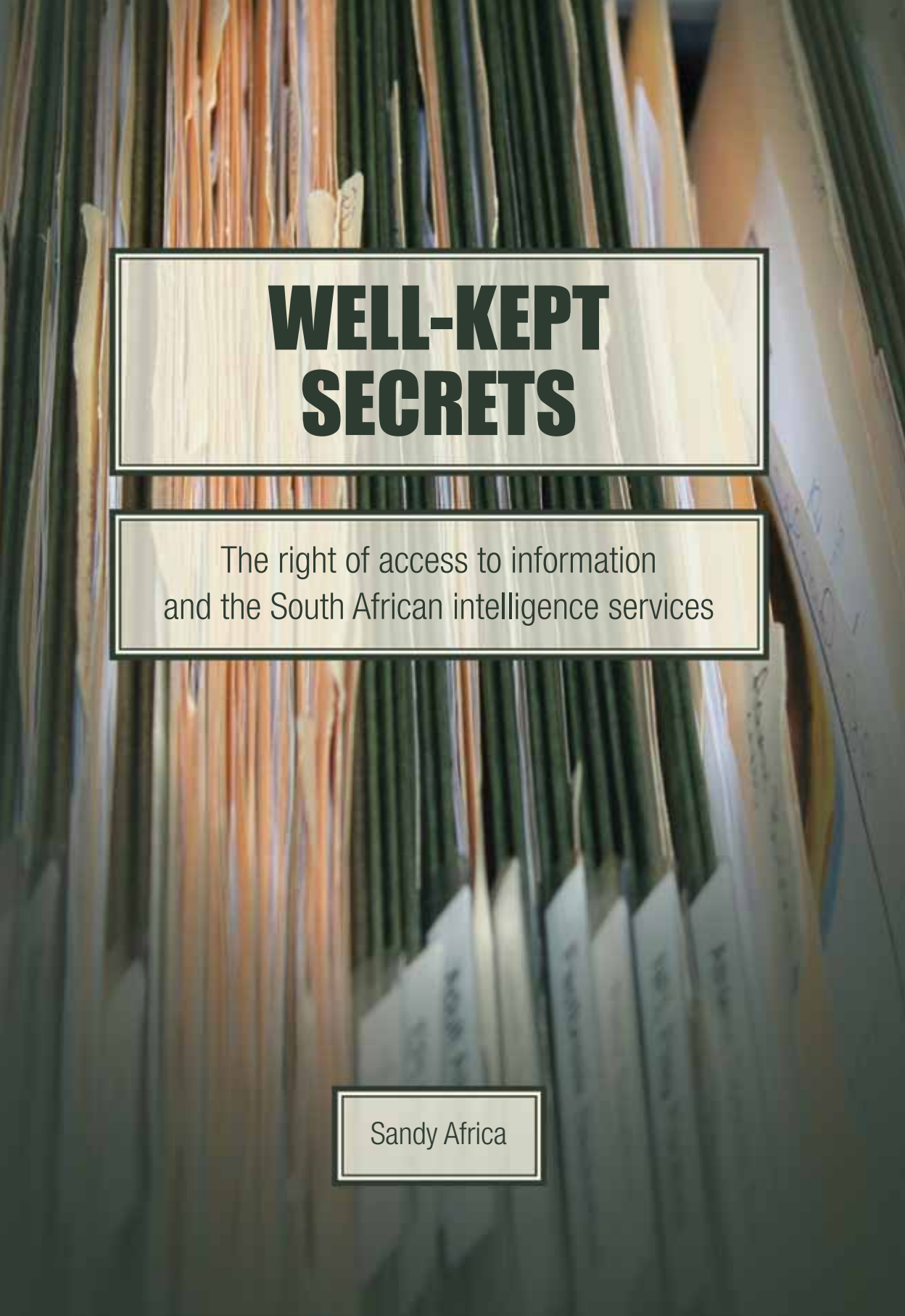

WELL-KEPT SECRETS

The right of access to information and the South African intelligence services

Sandy Africa

WELL-KEPT SECRETS

WELL-KEPT SECRETS

The right of access to information
and the South African intelligence services

Sandy Africa

Institute for

Global Dialogue

FRIEDRICH EBERT STIFTUNG

Jointly published by:

Institute for Global Dialogue
IGD House, Thornhill Office Park
Bekker Street, Vorna Valley
Midrand, South Africa
P O Box 32571, Braamfontein 2017
Tel +27 11 315-1299
Fax +27 11 315-2149
info@igd.org.za
www.igd.org.za

Friedrich-Ebert-Stiftung
Mozambique Office
Avenida Tomás Nduda 1313
Maputo, Mozambique
Tel: +258 214 912 31
Fax: +258 214 902 86
fes@tvcabo.co.mz

First impression in May 2009

ISBN: 978-1-920216-22-1

Designed and produced by Acumen Publishing Solutions, Johannesburg
Printed by Paarl Print

CONTENTS

ACRONYMS AND ABBREVIATIONS

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
CDRC	Classification/Declassification Review Committee
CIA	Central Intelligence Agency
CODESA	Convention for a Democratic South Africa
COSATU	Congress of South African Trade Unions
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
EU	European Union
FOIA	Freedom of Information Act
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
ISCOR	Iron and Steel Corporation
ISSUP	Institute for Strategic Studies, University of Pretoria
IRC	Interdepartmental Review Committee
JCIC	Joint Coordinating Intelligence Committee
JSCI	Joint Standing Committee on Intelligence
KGB	*Komityet Gosudarstvyennoi Biezopasnosti* (Committee for State Security)
MISS	Minimum Information Security Standards
NGO	Non-governmental Organisation
NIA	National Intelligence Agency
NCC	National Communications Centre
NICOC	National Intelligence Coordinating Committee
NIS	National Intelligence Service
NP	National Party
NSA	National Security Agency
NSMS	National Security Management System
OAU	Organisation of African Unity
OB	Ossewa Brandwag
PAC	Pan Africanist Congress
PAIA	Promotion of Access to Information Act, 2000
PFMA	Public Finance Management Act, 1999
PKO	Peacekeeping Operation
RCMP	Royal Canadian Mounted Police
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
SARS	South African Revenue Service
SASS	South African Secret Service
SIRC	Security Intelligence Review Committee
SSAC	State Security Advisory Council
SSC	State Security Council
TBVC	Transkei, Bophuthatswana, Venda, Ciskei
TEC	Transitional Executive Council
TRC	Truth and Reconciliation Commission
UDF	Union Defence Force
UDF	United Democratic Front
UN	United Nations
UNITA	National Union for the Total Independence of Angola
USA	United States of America
USSR	Union of Soviet Socialist Republics
WHAM	Winning Hearts and Minds

PREFACE

Civilian intelligence services are often perceived as occupying a recondite world, characterised by secrecy, ambiguity, and concealment. But not always understood is that they are subject to stringent oversight and accountability imperatives, which are often legally enshrined. Access to information is thus an important normative aspiration for any society that seeks to promote the virtues of democracy. One of these is the right of the public to know about the nature of intelligence work with regard to its policy, operational and regulatory dimensions. This takes on added meaning and relevance in defining the parameters of how political power is exercised and managed.

The case of South Africa is thus especially intriguing, interesting and important. The state's previous civilian intelligence apparatus occupied the dark recesses of illegality, where it helped to uphold and protect the apartheid regime and its security dictates. In the current dispensation, it has emerged into the broad daylight of being subject to public scrutiny, transparency, and democratic accountability. However, as the author trenchantly argues, this changed reality should not mask the persistence of awkward dilemmas, tensions and ambivalences in law, policy and practice. Indeed, these will continue to define the challenges highlighted in this enquiry, crucially given that the ruling party, the African National Congress, had its own intelligence systems and culture while conducting its struggle for liberation.

Rich in texture and nuance, judiciously balanced by the perspectives of a former practitioner and scholar, and informed by comparative experiences, this book represents a pioneering attempt to impose analytical and normative order on how constitutional prerogatives have shaped the interface between the civilian intelligence architecture and access to information in the first decade of South Africa's transition to democracy.

The Friedrich Ebert Stiftung and the Institute for Global Dialogue have come together in a collaborative spirit to make this publication possible. This is not only indicative of their recognising the value of this book but also reflects an abiding commitment to bring it into the public domain where it deserves a wide readership.

We take this opportunity to thank the author, Prof Sandy Africa, for her cooperation throughout as well as her dedication in updating the study with new and relevant material. The last word of gratitude is reserved for Riaan de Villiers who ably turned a doctoral dissertation into a highly engaging and readable narrative.

Manfred Öhm
Resident Representative
FES: Mozambique

Garth le Pere
Executive Director
IGD: South Africa

FOREWORD

This volume is based on my doctoral dissertation, and represents an attempt to make the study as accessible as possible to a wider audience. I hope it will be read by members of the South African intelligence services, past and present, and that they will find it a fair representation of the way in which the post-apartheid civilian intelligence dispensation came into being, and how the challenges that emerged in the course of that process have been addressed. I also hope it will be read by, and benefit, other policy actors – the executive, members of parliament, and members of human rights bodies – as well as students in policy and security studies.

Most importantly, I hope that members of the public, who may have been mystified or intrigued by the limited information about the South African intelligence services in the public domain, will feel inclined to explore this study. Certainly, members of the international policy community have displayed considerable interest in the South African model of 'security sector reform', the catch phrase for inclusive efforts to subject security institutions to universally agreed instruments of control, accountability, and oversight. Other African countries emerging from conflict have also displayed an interest in the South African experience, as have analysts and others in more stable societies with a renewed interest in the accountability of their security and intelligence institutions. I hope this book will enrich their enquiries.

Many people have contributed to its evolution. Professor Gavin Cawthra was an unassuming yet knowledgeable supervisor during the lengthy doctoral dissertation process. Several of my bosses in the intelligence services, including Tim Dennis, director-general of the South African Secret Service (SASS), and Lindiwe Sisulu and Ronnie Kasrils, ministers for the intelligence services, succumbed to my rather impertinent requests for sabbatical leave. Interviews and discussions were an invaluable source of information. I interviewed or held discussions with experts involved in drafting the Promotion of Access to Information Act (PAIA); officials of the Department of Justice and Constitutional Development, the lead department responsible for implementing the Act; the head of the South

African National Archives; constitutional and statutory bodies aimed at ensuring transparency and accountability, including the South African 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 senior officials of the intelligence services, on their implementation of the constitutional and legislative requirements for access to state information.

My own position as a senior manager in the intelligence services provided me with access to relevant officials and policy actors. At the same time, I often experienced a degree of tension between being part of the system and explaining away its failures, and adopting a more critical perspective with a view to stimulating debate and encouraging higher standards of accountability.

Colleagues, friends, and family members who shaped or shared my ideas, helped to source information, or commented on parts of the earlier dissertation included Verne Harris, Pingla Udit, Wayne Hendricks, Dennis Dlomo, Kerenza Millard, Rachmat Rassool, Lorna Daniels, Jennifer Brady, Howard Varney, Taki Netshitenzhe, Willem Hanekom, and Rieaz (Moe) Shaik. Siyabonga Cwele and Zola Ngcakani of the intelligence oversight community encouraged me to publish the dissertation. The late Joe Nhlanhla personified the new intelligence dispensation, and the framework crafted under his leadership and those of other visionaries across the political divide inspired me to persevere with the dissertation and this book, in a small effort to preserve the vision and idealism of the early efforts. These ideals have spread across Africa, where there is a steady but growing appreciation of the need for intelligence reform, and where South Africa's modest efforts in this regard are being emulated and even – with the benefit of hindsight – improved upon.

I received encouragement from many others, as well as space and patient biding at the University of Pretoria from Professor Maxi Schoeman. Moral support and encouragement were provided in generous amounts by my husband, Vejay; my children; my father and siblings, even as the end drew near for my terminally ill mother; and relatives and friends.

I am grateful to the Institute for Global Dialogue (IGD) for agreeing to publish the book, and to the Friedrich Ebert Stiftung (FES) for agreeing to finance it. I also wish to thank Riaan de Villiers, who expertly guided the conversion of a stiff academic dissertation into a more conversational, more readable, and hopefully more interesting text, and his team at Acumen Publishing Solutions for producing an attractive and easily readable book. At the same time, I remain responsible for whatever inaccuracies and deficiencies may remain.

A book on this topic begs the question of what impact intelligence has on the lives of ordinary citizens, and whether and how they should influence the debate on the role of these kinds of institutions. In the end, I am not sure whether I have answered this question. I argue the need for a comprehensive set of policy measures aimed at broadening the public's understanding of, and capacity to discuss and engage with the intelligence services. An informed public is the most effective way to ensure that state structures with such potent powers are held to account. I argue that such a policy should provide a clear framework in terms of which information should be protected from disclosure, or, to put it more directly, the conditions under which secrecy should be allowed. On the other hand, public policy should also provide clear criteria for deciding when information no longer requires such protection. While some would probably disagree, I argue that intelligence services have a legitimate role in South Africa's new democracy. The challenge is to ensure that they do not undermine the very democracy that their charters require them to protect.

Following decades of secrecy, promoting access to information is a relatively new experience for South Africa. 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 citizens to access information held by the state involves difficult choices. However, the history of unaccountable and secretive conduct on the part of South African security actors suggests that policy actors in government and elsewhere should continue to regard this as a national priority.

Sandy Africa
April 2009

32. Access to information

Everyone has the right of access to any information held by the state …

National legislation must be enacted to give effect to this right …

36. Limitation of rights

(1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom …

… Except as provided in subsection (1), or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights …

Extracts from the Bill of Rights, Chapter 2, Constitution of the Republic of South Africa

INTRODUCTION

In 1994 South Africa emerged from a period of minority rule characterised by excessive government secrecy and the denial of basic human rights. One such right was the right of access to information generated and held by the state. While post-apartheid governments have been far more transparent than their predecessors, policy-makers of the new political order have not reflected adequately on the implications of transparency for the intelligence services. Consequently, South Africa does not have an explicit and coherent policy on access to information about the intelligence services, or the information they hold or generate. Among other things, it is not altogether clear what information or records created or held by the intelligence services need to be protected, from whom, and why.

As a result of this policy vacuum, the post-apartheid intelligence services have been ambivalent about and inconsistent in applying the constitutional principle of the universal right of access to information held by the state, as well as legislation aimed at giving effect to it. One consequence of this is that citizens as well as organisations functioning in the public sphere do not always understand their rights in this respect; specifically, they often do not understand that the records of the intelligence services are in fact public records.

The concerned citizen, however, would want to know the following: what are the mechanisms for managing the records of the intelligence services? Are these filed safely and securely so that they can be retrieved when needed – for instance, when those services receive requests for access to information? Do the services actually know what records they have, and given the secrecy involved in intelligence, is it possible for them to know? Are the records tamper-proof? What is the retentions and disposals policy of the intelligence services, and under what conditions, if any, are records released for public consumption?

Another layer of questions relates to secrecy. Which documents are classified as secret or confidential, and why? Who takes these decisions, and under what authority? For how long may such documents be classified as secret, and what happens if this status is no longer necessary? Lastly, is there any oversight of what happens to these records, and how can the public be assured that their custodianship is in good hands?

BACKGROUND

Prior to 1994 the South African intelligence services were virtually immune from public scrutiny. The Official Secrets Acts of 1912 and 1956, the Security Intelligence and State Security Council Act of 1972, the Bureau for State Security Act of 1978, the Protection of Information Act of 1982, and various laws relating to the financing of the security services all served to draw a veil of secrecy around them (Mathews 1978; Africa 1992).

The post-apartheid constitution – which came into force in 1996 – established a number of institutions aimed at supporting a rights-based constitutional democracy. These include 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 (Constitution, 1996, chapter 9).

The statute book has been extensively revised to align it with the constitution. Hundreds of apartheid laws have been repealed or modified, and new laws adopted. Some provide for institutions aimed at promoting and upholding the Bill of Rights. For example, arising out of a constitutional provision, the Intelligence Services Control Act of 1994 provides for the establishment of a multiparty parliamentary oversight committee and the appointment of inspectors-general tasked with investigating complaints against the services by members of the public.

The new constitution also stipulated that national legislation should be introduced to give effect to the right of access to information held by the state, resulting in the adoption of the Promotion of Access to Information Act (PAIA) of 2000. This law requires state security organs to actively disclose information about themselves, and respond to requests for access to their records. However, some observers argue that the security services continue to resist disclosure, thus undermining the constitutional principle of access to information (Harris 2002; Currie & Klaaren 2002).

Gearing the post-apartheid intelligence services towards discharging their constitutional obligations to implement PAIA carries significant challenges in respect of capacity. The Act is relatively complex, and its implementation requires, among other things, the production of manuals; a capacity to respond in a timely fashion to requests for access to records; an 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).

In 1995 the National Intelligence Agency (NIA), the South African Secret Service (SASS), and the National Intelligence Coordinating Committee (NICOC)

were established, constituting the civilian intelligence sector. Since 2000 the sector has been significantly expanded with the formation of the South African National Academy of Intelligence (SANAI); Electronic Communications Security (Pty) Limited; the Office for Interception Centres (OIC); and the National Communications Centre (NCC). It is safe to assume that the secret records of the intelligence services have grown exponentially. Public ignorance and intelligence service ambiguity are 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, citizens must be assured that there are clear parameters and policy guidelines for the exercise of secrecy and transparency.

THE AIM OF THE STUDY

When one assesses whether the intelligence services have complied with their constitutional obligations in the first decade of their existence – that is, from 1995 to 2004 – it appears that both the services and relevant policy-makers have been ambiguous about how appropriate and meaningful levels of transparency should be pursued, and under what conditions the services may invoke a right to secrecy. A more pessimistic analysis would be that the way in which the intelligence services have retreated into justifications of secrecy even when greater openness and public disclosure would not have threatened national security, displays a significant continuity with the apartheid past. How are we to understand and explain this ambivalence, and present policy alternatives that will compromise neither the intelligence services' execution of their mandate nor the public right of access to information held by the state?

This study is based on the premise that the post-apartheid intelligence services are guided by the country's constitution, including its injunction on access to information. One should remember that the services themselves have been created in terms of the constitution, which indicates that its architects foresaw the need for entities whose functions would include the gathering of intelligence in pursuit of national security, presumably in the knowledge that they would carry over into the new dispensation those methods and practices – of intrusion, surveillance, and restrictions on access to information – that are inimical to the democratic ideal, but part of the realities of governance in the modern world. The conduct of the intelligence services would therefore have to be aligned with their status as constitutional entities, and the duties imposed by this imperative. This includes being

subject to the Bill of Rights, which guarantees the rights of free association and expression, privacy, dignity, life, and access to information held by the state. This is a challenging reality, but one which the South Africa polity and citizenry can be grateful for.

By way of background, and in order to improve our understanding of the current legal and policy environment, this study explores official secrecy in South Africa in the years of white minority rule. It traces the political imperatives that caused successive 20th century governments to introduce legislation that ensured their continued dominance over the country's black majority.

The study also assesses the state of access to information about the intelligence services in the period during which the country's negotiated settlement gave rise to a new intelligence dispensation. Once they began to discuss a new intelligence dispensation, the parties to the process – principally the National Party (NP) government and the African National Congress (ANC) – rapidly agreed on the strategies appropriate to conducting this type of work. Secrecy would be a necessary and unavoidable strategic imperative. Even though they might have been poles apart politically and ideologically, the main parties were united on the core issue of how the intelligence services should go about their business.

This study addresses the issue of whether the methods of secrecy employed by the post-apartheid intelligence services are legitimate and sustainable in a democracy, and whether sufficient safeguards have been put in place to ensure that abuses of power are avoided, or can at least be detected. As noted earlier, the intelligence services have been created under the constitution, and are subject to a number of democratic principles. In this regard, the first question is whether they operate under enabling conditions, whether their mandates and focus are clearly and explicitly spelt out in their founding legislation, and whether their efficacy is enhanced by the governance requirements imposed upon them. A second question concerns the impact of the seemingly contradictory policy, legislative, and regulatory arrangements under which the intelligence services function in respect of public access to information. The main contradiction is that, while the constitution confers a right of access to information held by the state, some organs of state (notably the intelligence services) are also directed to conduct their affairs in relative secrecy (Currie & Klaaren 2002). Thus the Intelligence Services Act of 2002 requires the heads of those services to protect the identities of members, sources, and methods of collection (Qunta 2004). And the Protection of Information Act of 1982, which has coexisted since 2000 with PAIA, 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 while the National Archives Act of 1996 provides for the declassification of records after 20 years, it does not state how records originally classified as secret on the grounds of national security are to be handled after the 20-year period (McKinley 2004).

The current situation is that information is classified in terms of a cabinet guideline, the Minimum Information Security Standards (MISS). What provides cause for concern is that while the MISS requires officials in all government departments, without regard for their levels of authority or responsibility, to adhere to its prescriptions for secrecy, it does not provide any oversight mechanisms. Officials are required to classify 'sensitive' information as 'Top Secret', 'Secret', 'Confidential', or 'Restricted', depending on the perceived degree of harm to national security should the information be disclosed (Currie & Klaaren 2002). The criteria for classifying records, and therefore for withholding information from the public, are not contained in any legislation, creating concern that the MISS in fact contradicts PAIA. This study explores the implications of these gaps in the legislative and policy framework, and recommends options for addressing them.

A third question is whether the custodianship of intelligence records is regulated in a way that guarantees their safety and integrity. This concern is particularly germane to information about – and records of – the intelligence services, because they are generally closed to public scrutiny (Posel & Simpson 2002). Members of these services are sworn to secrecy and may not disclose their activities; only a limited amount of information about the activities of these structures is released to the public, and even oversight bodies are often not at liberty to publicise all aspects of their interactions with these structures. Yet, as South Africa's own history demonstrates, it is precisely under such conditions that security forces and intelligence services can commit major misdeeds, all in the name of national security. Thus the Truth and Reconciliation Commission (TRC) – a body established by the first post-apartheid government to facilitate redress for politically inspired criminal acts committed under apartheid – emphasised the need for the preservation of official records in post-apartheid South Africa. Inter alia, it exposed the fact that the apartheid government had destroyed most of its records in its final months (TRC 1998). The impunity with which this was done serves as a reminder that whole chapters of executive action can be wiped off the slate, rendering state actors unaccountable and unpunishable for any misdemeanours.

The study raises the need to better characterise the security threats facing South Africa, and the kinds of intelligence information that should be kept secret as a result. It also raises the issue of who should have the authority to classify

information, and in terms of what criteria. It illuminates the challenge of finding a formula for preserving and handling the records of the apartheid intelligence services, especially in the context of processes to encourage disclosure about human rights abuses committed by the apartheid security forces. This will play an important role in bringing closure to that period in South African 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. Put differently, there should be safeguards to ensure that the classification or declassification of information is in the public interest, but these are either inadequate or do not yet exist.

LOCATING THE STUDY

Like their counterparts around the world, the South African intelligence services keep secrets – usually in the name of national security. More than any other department of state, they routinely withhold information from the public, and even from other government departments. As a result, members of the public as well as some members of the executive know relatively little about their activities, with the further consequences that misconceptions about them abound. Under these circumstances, the intelligence services tend to become defensive about their operations, and ambivalent about issues of transparency. This is one of the most significant challenges which post-apartheid South Africa must overcome.

In a democracy purporting to uphold the public's right of access to information held by the state, questions arise about when the non-disclosure of information is justified, and whether keeping these services going is an acceptable way of spending taxpayers' money. In their defence, the intelligence services lay claim to a professional duty of secrecy (to protect vulnerable informants, for example, or to preserve the confidential nature of intelligence liaison between states). They also point out that they are required by law to keep information secret under certain circumstances, at pain of criminal sanction. The reassurance that matters will not get out of hand, they claim, can be found in the country's constitution, which unequivocally states that the conduct of intelligence services must conform to the rule of law as well as international humanitarian law.

Policy analysts often assume that there is a causal link between governmental secrecy and the abuse of power – and, conversely, that greater public access to information, particularly about security and intelligence services, automatically promotes fair and judicious government (Halperin & Hoffman 1977; Richelson 1989; Steele 2001; Hodess 2003). In South Africa there is a growing expectation

that more and more information about the security and intelligence services will be made public, and that these bodies will be held accountable for their actions, both past and present (Africa 1992; Nhlanhla 1992; Harris 2000; Bell 2001; Klaaren 2002; Levy 2004).

Executive secrecy is generally frowned upon by citizens in a democracy, and in this sense intelligence services are not alone. Any form of official secrecy tends to create a climate of distrust between government and citizens, and that the cycle of governmental secrecy and public alienation are a feature of many western democracies. This cycle reproduces itself in the following way: 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, while government becomes increasingly frustrated by the simplistic analyses of the public whose opposition is perceived to be motivated by misunderstandings and simplistic and extreme responses (Mathews 1978).

Even where countries have enacted access to information legislation, it does not always mean that access is guaranteed. In many countries, enforcement mechanisms are weak, and governments often resist having to release information. Alternatively, bureaucrats delay the processing of requests for information (Martin & Feldman 1998). Not surprisingly then, around the world, intelligence services are increasingly closely scrutinised. Citizens and their representative institutions are asking their governments to explain what these institutions are contributing, especially in times when hard policy choices have to be made.

WHY THIS DEBATE IS IMPORTANT FOR SOUTH AFRICA

There are a number of reasons why this study is particularly relevant today. South Africa is a relatively new democracy, and even though the governance of its intelligence services been debated and scrutinised both before and after the first democratic elections, greater attention needs to be paid to detail. The debate about the tension between secrecy and transparency is part of a set of wider concerns about the accountability of security services in democratic settings. In turn, these concerns relate to how national security is conceptualised and advanced by a society and its government. The debate about national security has been influenced by the assumptions and world views of the different proponents. In the western world, conceptions of national security were an important dimension of international relations theory during the Cold War.

The main objective of the two leading protagonists – the United States and

the Soviet Union – was to gain the lead in the race for strategic global dominance. Intelligence services – notably the Central Intelligence Agency (CIA) and Committee for State Security (KGB) – played a prominent role in the conflict. Intelligence services of other countries throughout 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 communist East bloc countries from extending their influence, particularly in the third world, and ensuring that western countries remained ahead in the nuclear arms race. In the 1960s the generation of intelligence information proliferated, with western powers spending massive sums on developing technologies to give them an advantage in the spy wars against the Soviet Union.

Africa did not escape these alignments. Modern African states had their origins in the colonial partitions that 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 Europeans were mainly designed to facilitate access to the continent's abundant natural resources. National identities were imposed on Africans, with historically specific identities and the heterogeneity of African societies being ignored or misunderstood. Very often, the only unifying factor in a given colony was the fact that it was subject to a single colonial power. Ironically, the common experience of colonial oppression gradually created a sense of nationhood among the people forced together in this way, resulting in the formation of resistance movements, and demands for independence from colonial rulers (Smith 1983).

When independence came, however, many of the colonial administrative structures remained intact, or served as models for the new post-colonial states. Post-colonial intelligence services often merely reflected core–periphery relations, even after nominal independence from colonial powers had been attained. South Africa's democratic transition coincided with the post-Cold War era, and the intelligence services therefore had an ideal opportunity to effect governance arrangements that put accountability and professionalism before ideology. This study will hopefully show the extent to which the intelligence services were able to adhere to these principles in the first ten years of their existence.

The study also comes at a time when numerous democracies threatened by violence and extremism are thinking about restricting their citizens' civil liberties in the interests of national security (Todd & Bloch 2003). During the 'War of Terror', the United States, followed by several western countries which prided

themselves on their civil liberties credentials, extended their intelligence services' use of secret, intrusive and, it was widely suspected, illegal methods. The debate on how much secrecy a society should tolerate is particularly pertinent to South Africa, given that, having emerged from a past in which the state disregarded human rights, any reversal or even qualification of the fundamental rights provided for now will be subject to the test of constitutionalism. This study recognises the human rights underpinnings of the post-apartheid security dispensation, and attempts to find policy solutions within this paradigm. The debate around access to information held by the state is taking place at a time when rapid technological development, and an information explosion have exposed 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 they cannot guarantee that the information they collect and store is invulnerable to unauthorised access (Lipinski 1999). This affects the durability and efficacy of secrecy regimens, and calls into question the funds needed to secure information systems and personnel entrusted with information security.

Another factor affecting the efficacy of secrecy systems is globalisation, and the growth of multinational governmental and private entities. Identities are increasingly defined in transnational terms, and individual loyalty to a country might exist alongside or even be surpassed by identification with multinational corporations. The implications of this phenomenon – which is dramatically facilitated by new technology – is that people are increasingly identifying with causes regardless of geographical boundaries. In a technologically linked global environment, where access to information is often the key to prosperity, and territorial identities are being subsumed by other forms of identity, actors who have to develop appropriate policies for promoting and defending national security face major challenges.

Finally, the study is relevant because it explores the interplay between various policy actors in the course of providing access to information. These include the executive, parliament, officials of the intelligence services and other related departments, oversight bodies, and organs of civil society. While they broadly agree on principles, they often have divergent interests, which leads to differences in interpreting and applying policy. I conducted interviews with some of these actors, including officials in the intelligence services and other government departments, drafters of the legislation promoting access to information, members of various oversight structures, academics, and representatives of NGOs. Understanding the perspectives of policy actors – where they converge, and where they differ – is an important part of the policy-making process, which must seek

to manage these tensions in the interests of the various stakeholders (Lee 1991). The concluding policy recommendations represent something of a balancing act, and recognise that most or all divergent views are partly valid.

THE SCOPE OF THE STUDY

The terms and definitions used in respect of South Africa's statutory security institutions are derived from the constitution. Chapter 11 of the constitution refers to 'security services', comprising the national defence force, the police service, and the intelligence services. The actual shape and functions of the intelligence community were the product of extensive debate between the parties involved in negotiating South Africa's political future in the early 1990s.

One of the major departures from the apartheid dispensation was to establish two civilian intelligence services, one for domestic intelligence and another for foreign intelligence. Under apartheid the premier civilian intelligence service was the National Intelligence Service (NIS), which collected both domestic and foreign intelligence. In addition, the 'Bantustans' of Transkei, Bophuthatswana, and Venda had their own intelligence services. Modelled on the NIS, they largely concentrated on flushing out anti-apartheid activists, and relied heavily on Pretoria for direction and resources. When the intelligence services were amalgamated in 1995, the members of these satellite services were also absorbed into the two new services.

In line with the White Paper on Intelligence and National Strategic Intelligence Act of 1994, the mission of the domestic intelligence service – the NIA – is to conduct security intelligence within the borders of the Republic of South Africa in order to protect the constitution. Its aim is 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 detrimental to the national stability of the republic, or threats or potential threats to the constitutional order of the Republic and the safety and well-being of its people. The mission of the foreign intelligence service – the SASS – is to conduct intelligence in relation to external threats, opportunities, and other issues that might affect the Republic, 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 to formulate foreign policy (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 to those sectors of the security services. There is room for broadening the analysis in this area, not least because the intelligence community straddles the defence and policing environments (Africa & Mlombile 2001). This is made clear in the National Strategic Intelligence Act of 1994 which outlines the strategic intelligence-gathering mandates of the NIA, SASS, Defence Intelligence, and Crime Intelligence.

This study focuses on policies and policy alternatives for managing intelligence information, defined as records generated by the intelligence services in the course of their work. These include the raw information documented and compiled from a number of sources, including informers, technical and signal collection points, written reports, and analyses compiled by intelligence officers; and the assessments and reports generated from this data, usually assessments of threats or perceived threats to national security presented to policy-makers (Richelson 1989). It also includes dossiers on people and organisations, and records of the methods used to gather the information in question.

The definition of intelligence records also covers records about governance of the intelligence services, including human resources, assets, and financial management. '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 used to evaluate it.

The study also explores issues around the status, legitimacy, and ownership of intelligence information in the country's movement from authoritarian to democratic rule. As a backdrop it reviews and assesses the political processes leading to the establishment of the new intelligence dispensation, notably the formation of the NIA and SASS, which were to function under a changed set of political rules. A core focus of this study is whether, in the course of their formation and early development, they have adapted to these rules of accountability and regard for the constitution and the law.

It seeks to analyse how, in post-apartheid South Africa, all three arms of government – the legislature, executive, and the judiciary – as well as officials of the intelligence services have defined their relationship to intelligence information 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 – interact with the intelligence services in line with their respective mandates. Their record in playing these oversight roles is briefly reviewed. It is widely known, and even accepted, that the intelligence services do much of their work in secret, giving rise to the central dilemma exercising this study: how credible policy can be made 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 that make it possible.

Finally, it examines the experiences of several countries that have grappled with the issues of maintaining a successful balance between transparency, secrecy, and national security in managing their intelligence services. Oversight mechanisms have played a prominent role, especially in the West, and form an important part of the democratic armoury against bureaucratic excess. It would obviously have been valuable to compare South Africa's experiences in this regard with those of other African countries, but few seem to promote access to the records of their intelligence services in a similar fashion. Given this, developed, largely western countries had to be examined. While the choice of countries is not exhaustive, and their experiences cannot be directly compared with South Africa's, they do offer insights into how civil society and security establishments in various societies have differed on these issues, and how policy-makers have intervened to resolve disputes and demarcate the boundaries more clearly.

Ultimately, this study seeks to contribute to public policy. It identifies a need for effective policy responses to the enduring problem of balancing secrecy and transparency in intelligence work, and suggests how such policy should be evolved, implemented, evaluated, and adjusted. In the process it draws on several academic fields – law, history, philosophy, politics, and international relations – which is not unusual in the area of policy studies (Lee 1991; Dunn 1994; Parsons 1995).

Heymans (1996) has offered this common-sense definition of the role of public policy:

> The business of government is to make choices, and to strategically manage resources towards achieving the goals these choices imply. Public policy is the product of these choices, setting the parameters within which government departments and others operating within the sphere of particular polices are either intended or made to function.

Setting out the challenges of policy-making in a democracy such as South Africa, he spells out three attributes that must be present for government to make, analyse, implement, and evaluate policy:

> … political leadership (to make choices and take responsibility for their outcomes); administrative management (to make things happen); and analytical support (to identify, explore and package policy-relevant options and information) (Heymans 1996:30).

This study fundamentally interrogates a policy problem: how much information should governments in general and the South African government in particular make available to the public, or, conversely, how much information is it entitled to withhold from the public domain? If information about the security of a country and its people is a public matter, are policy-makers making appropriate choices about access to such information; and how are these choices being interpreted and implemented by the bureaucracy and the intelligence bureaucracy in particular?

STRUCTURE

This book is divided into three parts. Part One provides a context for and background to the rest of the study, and deals with conceptual issues relating to secrecy and transparency in the governance of intelligence services; official secrecy prior to 1994; and the transformation of the intelligence services in the course of the transition to democracy.

Part Two deals with the new security dispensation; more specifically, it deals with statutory instruments facilitating access to information about the intelligence services; as well as PAIA and its implications for the intelligence services. It also reports on two court cases and a commission of inquiry centring on the intelligence services and the right of access to information.

Part Three concludes the book with lessons from international experience, conclusions, and policy recommendations.

PART ONE

Context and background

1

SECRECY AND TRANSPARENCY IN THE GOVERNANCE OF INTELLIGENCE SERVICES

IN SOUTH AFRICA, as in other societies around the world, secrecy arises in various social contexts, presenting a range of political, legal, and ethical dilemmas. Some of these dilemmas are universal, and have been with us for a very long time. Medical secrecy, as embodied in the Hippocratic Oath, obliges doctors to treat disclosures by patients as confidential. The legal profession too must contend with the dilemma of secrecy. Strauss describes this as follows:

> Attorneys and advocates are ethically bound in the same way as a doctor or priest to maintain confidentiality in regard to information disclosed to them in confidence by their clients. Failure to comply with this duty can result in disciplinary action being taken against the legal practitioner … in the technical sense of the word, it can be categorised as 'a right to unfettered freedom from the state's coercive or supervisory powers and from the nuisance of its eavesdropping'. Although generally known as a legal professional privilege, it is really a right which the *client* has to withhold from a court of law communications made to his lawyer, and to prevent the latter from disclosing such communications as evidence (1983:26).

A third area in which issues of secrecy present themselves is journalism. Journalists are sensitive to an expectation of trust, and are often prepared to defy the authorities in order to protect their informants. Matthews attempts to describe what is common to all three of these areas of social interaction:

> The lawyer and his client, the doctor and his patient, the journalist and his informer, the corporation managers and the Government may all reasonably claim the protection of the law for certain communications or information. In each case the fundamental rationale for secrecy is that inability of the individual or institution to function effectively without legal guarantees against disclosure. But there is another common factor of equal or greater importance, and that is that in each case the interest in secrecy or non-disclosure is at best a qualified interest. The matter may be expressed differently by saying that in every instance the claim that secrecy should be maintained is opposed by a compelling claim favouring disclosure or access to information. … The law's task is to reconcile the opposing claims by demarcating the legitimate boundaries within which each is sovereign, and by determining when and to what degree the one may be limited in the interests of another or others (1983:36).

The American-Scandinavian philosopher Sissela Bok addresses the ethical and philosophical dimensions of secrecy in her book *Secrets – on the Ethics of Concealment and Revelations* (1982). She offers 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 it. Despite this supposed neutrality, secrecy is usually underpinned by socially influenced choices. Bok describes some of the social contexts in which secrecy might arise or be applied, including medical research and practice, secret societies, trade negotiations, research, and military and state activity.

According to Bok, secrecy can be utilitarian and justifiable. One example is withholding sensitive information from children. Another is withholding information from participants in research projects – such as which participants in a medical trial have been issued with a placebo. A third is restricting information to participants in sensitive trade or commercial talks if disclosure could affect the outcome to the detriment of either of the parties.

This raises the issue of when secrecy can be regarded as acceptable, and when not. According to Bok, the test should be whether the reasons can be convincingly defended in public. Moreover, the criteria for secrecy should never require concealment. In this regard, Bok 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. She argues that the secrecy surrounding matters of state are often simply an excuse to wield excessive power, and that the rights of the public are severely restricted when this is the case.

Bok's book about secrecy follows an earlier analysis of a related subject, entitled *Lying – Moral Choice in Public* (1978). In this work, she attempts to demonstrate that lies and deception could arise or be applied in a number of social contexts, and that their impact has to be assessed in this context. Contexts for lying include white lies (usually considered to be harmless); lying to enemies (tactically applied in a state of war); deceptive methods of social science research; and paternalistic lies (concealing an unpleasant truth from a child, or deception of the terminally ill about the state of their health). She argues that the consequences of truthfulness or deception should be carefully considered, whenever such a choice has to be made, but accepts that major dilemmas may arise in exercising this choice. She notes that an orderly social system depends upon a reasonable degree of truthfulness, and suggests that the truth should not be unduly subverted. The social costs of lying, she warns, include a disproportionate and unfair denial of power to groups which are already disempowered due to their lack of access to reliable information. As a result, the disempowered are unable to make appropriate choices to further their own well-being. In addition, the victims of lies are forced to carry a psychological and emotional burden of uncertainty.

Bok's works are relevant to our enquiry because they prompt us to confront the complexity and consequences of secrecy and confidentiality. Intelligence services keep secrets, and engage in processes that can be construed to be deceptive – both in the name of national security. Where they have been established by constitutional injunction, this makes for a fascinating subject. The South African constitution, to be sure, is silent on the methods to be used by the intelligence services, though it states categorically that these methods must be lawful, and consistent with the rule of law, including international humanitarian law. Yet the intelligence services would claim to have a professional duty of secrecy necessitated, for example, by the relationship between secret human sources of information and the services, and the confidential nature of intelligence liaison and exchanges of information between states. In addition, even in democratic states, such secrecy is specifically provided for in law, its breach carrying the burden of criminal sanction.

Robertson (1999) has also written about the policy question of secrecy, this time in respect of the security establishment in the United Kingdom. In fact, he has criticised Bok's work on the grounds that it does not provide any convincing criteria for judging when secrecy has become excessive. This diverts from her stated goal of a neutral approach to secrecy when addressing the role of the state. He accuses her of all but condemning the state for having ignoble intentions whenever it conducts its affairs in secret, no matter what the purpose may be:

> 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 1999:12).

Robertson's objection to Bok's assumption that secrecy in government is generally bad for society is relevant to our study. The intelligence services in democracies – including the United Kingdom – are typically required by law to conduct their operations in secret. Where there are checks and balances on their powers, as exercised through oversight mechanisms, Robertson argues that it is simplistic to conclude or assume that they will abuse their powers. He laments the fact that Bok, who has made the case for secrecy in other spheres of life so competently, has not been able to provide a more balanced account of its utility when exercised by the state.

Robertson is concerned about the impact of secrecy and its potential to turn democracies into 'surveillance societies' in which citizens are continually scrutinised by the state. He is however, equally cynical about the effectiveness of freedom of information laws – or 'access to information' legislation, as it is otherwise referred to – as a vehicle for open government, and facilitating meaningful insight into policy matters to the ordinary citizen. For Robertson, freedom of information legislation in many countries has been introduced in response to crises precipitated by government excesses, and serves to streamline the channels of communication between the public and the state rather than opening up avenues for influencing decision-making. He argues that restricting the processes through which information held by the state can be accessed is, ironically, potentially immobilising to citizens. Even though those in power must consider requests for information held by the state from members of the public, they are in a very powerful position, and information inadvertently becomes a lever of power. Moreover, they tend to release information only when requested rather than building and promoting a general culture and climate of openness.

The one advantage of access to information, Robertson concedes, is that it helps to ensure that records are more accurate, which benefits governments; and fairer, which benefits citizens. This is especially true of personal records retained by governments, and which citizens might be entitled to review through access to information legislation. However, he warns that:

> 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 (Robertson 1999).

This analysis cautions us against regarding access to information as the only measure of accountable and open government. Along with entrenching the right of access to information, the South African 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 judiciary; the establishment of parliamentary oversight committees; and the independent auditing of the financial statements of all government departments (RSA Constitution, 1996). Any assessment of accountability of the intelligence services must therefore take into account how these institutional measures are applied in relation to them.

Some 20 years ago, Anthony Mathews, a South African constitutional expert, considered the impact of secrecy on western governments as a backdrop to his seminal study *The Darker Reaches of Government: Access to Information about Public Administration in Three Societies* (1978). He argues 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 of the system of democracy. For Mathews, extensive secrecy in the executive branch and its departments is incompatible with democracy; however, the evidence points to the growing might of bureaucracy 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 (Mathews 1978).

Mathews argues that official secrecy create a climate of distrust between government and its officials on the one hand, and citizens on the other. The cycle of governmental secrecy and public alienation are a feature of many western democracies. This cycle reproduces itself as follows: 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 misinformation sets in, even where this is not the case, while 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'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. Because of this state of affairs, misconceptions about the intelligence services abound. Hardly surprisingly, the intelligence services have become increasingly defensive and ambivalent about meaningful transparency. This alienation of the intelligence services is one of the most significant challenges facing the post-apartheid South African state.

All three writers – Bok, Robertson, and Mathews – make valid points. Bok correctly argues that secrecy is not always a social evil, and that there may be conditions under which it should be accepted. This is evident from the examples she cites: the right of confidentiality of personal medical records; client–lawyer privilege in legal proceedings; and journalists' protection of their sources, to recall a few. Even lying and deception may be justified and socially acceptable in certain contexts, including the element of surprise, stealth, and secrecy often required in times of war; or declining to disclose the terminal nature of an illness to a relative. In similar vein, it can be argued that at least some secrecy and deception in respect of intelligence may be justified.

Bok's warning that state secrecy could be used as a cover for the abuse of power has proven to be prophetic too often in recent history, and this is the case with many of the scandals associated with intelligence services: they happen under cover of secrecy, and the inability of the public to object to questionable activities before it is too late. Yet Robertson believes that Bok has not shown convincingly enough that secret government is worse than open government. At one stage he even points out that she has conceded that good administration requires a degree of secrecy: for deliberations, for timing, and to maintain the confidence of those who have exchanged information on the understanding of confidentiality. The fact that Bok concedes that she does not have an answer for the questions of who should determine that secrecy is necessary, and for how long, does not make them go away, so it is just as well that she has raised them. These are difficult issues, and the only way to resolve them is to make policy choices and evaluate them

after a period of implementation, in order to assess whether they have helped to ameliorate the problems they set out to address.

Finally, Mathews has been prophetic in the way in which he has foreshadowed the dilemmas of the post-apartheid bureaucracy. The classical scenario of the bureaucracy as a generator of secrets, fuelling suspicion, and alienating itself from the public which it sets out to serve, is the very precipice that is the concern of this book. Mathews effectively juxtaposed the situation in respect to secrecy and access to information in apartheid South Africa to that in Britain and the United States. South Africa has now caught up with these countries; it is a democracy with a constitution endorsed by a representative parliament, and in which all citizens have the right to political participation. It also has a constitutional provision in respect of access to state information, and legislation on this subject that is binding on the intelligence services. The question that must be considered is whether this factor makes the intelligence services more transparent than in 1978 when Mathews wrote his book. In other words, it is a question of whether the transparency requirement has made a difference to the quality of intelligence governance, and whether this in turn has had an impact on the effectiveness and accountability of the intelligence services. In addition, the question that arises is whether the requirement of transparency is sufficient, or whether there is need for further instruments to ensure accountability.

BALANCING SECRECY AND ACCESS TO INFORMATION IN INTERNATIONAL RELATIONS

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), and several international covenants which promote freedom of information subject this right to certain qualifications. Evatt (1999) points to the International Covenant on Civil and Political Rights (ICCPR), adopted by the United Nations (UN) in 1966. Article 19 of the ICCPR guarantees freedom of opinion and expression, but subjects these rights to certain restrictions, including the protection of national security or of public order.

Evatt 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. Its effects

seem to have been minimal in real terms, at least in the area of freedom of expression. At best the Human Rights Committee of the UN 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).

The European Union (EU) is another example of a supranational authority whose instruments are binding on all member states. While the EU is said to be founded on four freedoms (of movement of persons, capital, and goods and services), each interest may be curtailed in the interest of national security. Moreover, Nichols (1999) informs us that, under the Treaty of the EU, no member state is obliged to supply information if such disclosure can be considered to be contrary to its security. Also, any EU member state may take any steps it considers necessary to protect 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 co-operative governance. The African Charter on Human and People's Rights (the African Charter) was accepted by the majority of members of the Organisation of African Unity (OAU), and its African Commission of Human and People's Rights was made responsible for supervising the charter. However, like the ICCPR, its impact has been limited. Chapter 9 stipulates that every individual shall have the right to receive information, and express and disseminate his opinion within the law. Nevertheless, this requirement is not carried over in the national legal frameworks of many African countries, and where it is, the practice is often very different to what is spelt out in law.

Secrecy is recognised as having a legitimate role in the international political system. Intelligence is therefore regarded by states, and international and intergovernmental bodies such as the UN, EU and AU, as being as relevant as ever, if not more so today than previously. In an increasingly uncertain world, even multilateral institutions such as the UN are considering the role of secret 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 seems to be coming to the conclusion that it does after all, require a secret intelligence capacity. Dorn (1999) makes a strong argument for UN secrecy, particularly where the success of a UN peacekeeping operation (PKO) may depend on secrecy and early warning gained through intelligence-gathering. He argues:

> Secret intelligence is even more important in modern multidimensional PKOs 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 (ibid: 3).

Dorn (1999) is concerned that the UN does not have any guidelines to deal with sensitive information, and that the variances in the information management systems of individual PKOs 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 created 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.

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.

ACCESS TO INFORMATION AND POLITICAL POWER

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 government 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; Paraschos 1975; Turner 1986; Shulsky 1991; Halperin & Hoffman 1977). Some of these 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 is addressed by Turner (1986), who points out that the reason the United States government introduced measures to counterbalance secrecy with transparency measures in the 1970s and 1980s was its experiences of unacceptable conduct within the security services, especially the intelligence community.

Some writers have argued that a lack of openness has fuelled 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 about 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.

The way in which 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; D' Souza 1999). Banisar (2002) cautions that the mere existence of access to information legislation does not always mean that access is guaranteed. In many countries, enforcement mechanisms are weak and governments often resist releasing information. Alternatively, bureaucrats delay the processing of information requests (Martin & Feldman 1998).

Intelligence services have undergone significant changes in the post-Cold War period, particularly in their relations with their countries' own citizens, and one would assume that this would mean greater access to information about the intelligence services, if only about their past. Yet the picture has been a mixed one. Many studies 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 countries where this has occurred has played a significant role in revelations about the role of intelligence services. Nevertheless, full disclosure remains a problem, even for bodies constituted at the instance of the state. Hayner (2001) writes about the difficulties that truth commissions often encounter in accessing official records of former repressive regimes. Some states undergoing transitions have been able to fill the information gap by accessing declassified records of other states, where there have been gaps in their own records. In the case of both 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-government 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 United States government, co-operation 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 American government's relations with these states, and providing insight into the role of the American intelligence services in the 1960s and 1970s.

This factor and these strategies – access to the declassified records of former authoritarian regimes – may be particularly relevant to South Africa, in view of the apartheid experience of the destruction of intelligence records. As revealed during the hearings of the TRC – initiated through a law of parliament to uncover gross human rights violations that had been committed during the apartheid period – the preservation of official records is at the heart of preserving national memory, yet huge volumes of records were systematically destroyed as the apartheid years drew to a close.

Measures of redress that may be chosen by states in the aftermath of periods of atrocity are often dependent on access to reliable records. This is the context in which the need to preserve them for posterity as public records, and not have them regarded as the exclusive property of any one agency, must be seen. 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.

THE ARCHIVES AND INTELLIGENCE RECORDS

Hamilton (2002) and Petersen (2002) have questioned the traditional conception and role of state archives. State archives, they argue, reinforce the isolation and secrecy of information: once buried in the archives, records in a way no longer exist, except for those who are its immediate custodians, and others who develop some arcane interest in it. They warn that state archives can falsely construct the past through the control of selection, description, and access to information. As a result, historians have been cautious about relying exclusively on public and more specifically government records. This is especially the case in South Africa, where archives are perceived to reinforce colonial and later apartheid biases.

The reconstitution of the archives in post-apartheid South Africa creates an opportunity to redress this legacy. The most important challenge is to incorporate the experiences of diverse stakeholders. Archives should therefore not only reflect how states want history to be recorded; they should also express the documented struggles and experiences of all the peoples within a common political space, irrespective of whether records have been captured by the state or not.

This brings us to the question of the duty of the state to preserve public records, and facilitate the preservation of non-governmental records. In South Africa, the records of the intelligence services have been particularly vulnerable to disposal on political whim, as happened in the closing days of apartheid when state records were destroyed under the direction of the state's intelligence services. This destruction of records continued well into the first years of the new democracy, a clear sign that the paradigm had not changed, despite the fact that those records were a clear link to the past that still needed to be understood and assimilated. Moreover, Pigou (2002) recounts the difficulties in gaining access to official information encountered by the investigation unit of the TRC, and claims that the SAPS, SANDF and NIA, to varying degrees, blocked access to the records of their predecessors.

These perspectives on the state 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 is that we should be careful not to mistake the state's record or version of reality as the final reflection of the 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 continuing to marginalise less powerful groups in society.

The second lesson arising out of this debate is the need to seriously reconsider how to improve access to state records and archives, and 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 in the shadows is a huge challenge. This study will deconstruct the implications of access to information about or from the intelligence services. Presumably, any information that falls outside the scope of one of PAIA'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.

ACCESS TO INFORMATION AND THE LAW IN CONTEMPORARY 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 predating the new constitution. Some analyses centre on 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). All these analyses attempt to apply or to establish legal principle in resolving contradictions between society on the one hand (either as a collective or the individuals therein), and the state or its institutions on the other.

The introduction of a Bill of Rights, both in the interim constitution of 1993 and the final constitution of 1996, 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 these writers have considered the implications for the policy and judicial landscape of the introduction of a constitutional right of access to information.

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 the apartheid era, during which secrecy was used to cover governmental excesses (Mathews 1978; Currie & Klaaren 2002; Levy 2004; Qunta 2004; Steytler 2004). Post-1994 analysts are concerned that society should not revert to that

dark past. An unintended consequence of this concern may well be that, while the case for transparency is compellingly made, the case for legitimate secrecy may be neglected.

CONCLUSION

Managing the tensions between secrecy and transparency in a democracy is often a complex task. The entrenchment of a constitutional right of access to information has been a defining feature of the post-apartheid political landscape, and chimes 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). While 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 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.

Most writers on the subject agree that transparency can be leveraged to give citizens access to information they need to defend their rights, and to give marginalised groups meaningful insight to the workings of state (Mathews 1978). However, as Robertson (1999) points out, access to information legislation around the world has not resulted in significant shifts in power relations, and must lead us to consider whether this alone is a sufficient requirement for accountable and transparent 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 internal or external conflict, it does not need to 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 that there is still a variety of threats for which the early warning capabilities of intelligence services are required.

Important work has been done around the significance of access to the records of fallen authoritarian regimes, when this becomes possible under a change of government. Such access has 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 TRC revealed a systematic destruction of state records. 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 that continue, after apartheid, to be subject to considerable control and secrecy. Opacity around state information holdings which are not readily accessible to the public raises the spectre of 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.

2

THE POLICY FRAMEWORK FOR OFFICIAL SECRECY PRIOR TO 1994

THIS CHAPTER EXAMINES THE policy framework for official secrecy under white minority rule. The period under review begins at the turn of the 20th century, and ends in February 1990 when the ANC, South African Communist Party (SACP), Pan-Africanist Congress (PAC), and other anti-apartheid organisations were unbanned. In this period, successive white regimes attempted to maintain their political and economic dominance, and entrench a racial notion of South African citizenship.

Five phases seem to define shifts in the state's approach to security. Prior to Union in 1910 both Boers and Britons established institutions aimed at warning them timeously of threats to their interests. The next phase starts in 1910 when South Africa's four white-controlled colonies were unified under a central government that owed its allegiance to the British crown, and continues to the end of World War Two. The next phase, following World War Two, covers the period when the Afrikaner-based NP rose to power, and began to consolidate racially exclusive and segregationist policies. The next phase starts with the banning of the liberation movements in 1960 and their subsequent resort to an armed struggle, and ends with the Soweto uprising in 1976. Excessive state secrecy, along with the suppression of civil liberties such as freedom of expression, association and movement, were fundamental pillars of white minority control. The last phase covers the period of mass political resistance, heightened state repression, and deepening political crisis in which the apartheid government began to realise that it needed to negotiate a political settlement with the liberation movements (Gerhardt 1978; Davidson et al 1976; Magubane 2004).

This study of official secrecy policy under minority rule examines, for each period, the policy imperatives of the governments at that time, the legislative framework, the administration of the system of secrecy, the shape of the intelligence and security forces, and the ensuing resistance against secrecy and repression. It is meant to provide a background to the post-apartheid secrecy system, sketching the origins of contemporary policy as well as its flawed political foundation, which helped to create its legislative and administrative shortcomings. Although it starts at the beginning of the 20th century, the apartheid era is emphasised, since it was the legacy of successive apartheid governments that had to be undone when democracy was formally attained in 1994.

THE PERIOD PRIOR TO 1910

The white regimes in the territories that later constituted the Union of South Africa believed they faced sufficient hostilities to justify the use of secret agents. Blackburn and Caddell (1911) captured the mood in which secret service first took root in colonial times:

> 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 (1911:3).

According to these authors, secrecy and espionage in this period dealt with issues that went to the heart of control over resources and the subjugation of indigenous people: the illicit liquor trade, gun running, and the smuggling of precious minerals. Regarding the formation of a Boer secret service, they describe the role of Dr William Leyds, Secretary of State of the Transvaal Republic, as central. After completing his legal studies in the Netherlands, Leyds, a brilliant student, was recruited by a scout who recommended him to President Paul Kruger. The Dutch were very sympathetic towards the Boers during their wars against the British,

a sentiment shared by Leyds, who did not hesitate to take up Kruger's offer to assume the post of prosecutor in the Transvaal (Van Niekerk 1985).

Leyds soon rose to the position of Secretary of State – a pivotal position in Kruger's executive. Under Leyds's guidance, a highly organised secret service was established:

> 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 … a separate account [was] voted and kept for '*informatie*'. Within ten years the secret service of the Transvaal developed from a primitive affair of private inquiries ... into one of the most expensive and extensive in the world (Blackburn & Cadell 1911:237).

A charismatic figure, Leyds placed great store in effective communications, and developed an extensive network of contacts in the European media, thus seeking to influence opinion in favour of the Transvaal Republic. He and other members of the Transvaal government probably had a similar outlook to that which held sway in the British Empire – then the most powerful in the world – which maintained an extensive network of informants to ensure that the Crown was well informed about all developments in its far-flung realm.

Official secrecy in modern South Africa can therefore be traced back to the period preceding the formation of the Union of South Africa in 1910 under the South Africa Act of 1909, which was passed by the British parliament (Bindman 1988). The unification of the two former Boer Republics (the Transvaal and Orange Free State) with the British colonies of the Cape and Natal was preceded by a national convention at which delegates sought to agree on how whites from various language groups could coexist while excluding blacks from the rights of citizenship. The exclusion of blacks from the Union's political and economic mainstream formed the core of the domestic security policy of successive white governments. They sought to manage the demands of white workers, while continuing to exclude the black majority from economic benefits, often using organised force to uphold this strategy.

FROM 1910 TO 1948

In this period, the Union was subject to British legislation on official secrecy. An Official Secrets Act was first passed in Britain in 1889, and superseded in 1911 by an amended Act. According to Mathews (1978), the Act might have been a

response to leaks of official documents about foreign affairs, including a secret treaty between the United Kingdom and Russia in 1878. The law prohibited British citizens from disclosing state secrets; thus the basic crime it created was the communication of official information and not espionage.

The English law, in the form of the Official Secrets Act, 1911 was applied in South Africa. This law was generally applied in British dominions, such as Australia, New Zealand and India in the early 20th century (Mathews 1978; Geldenhuys 1984). After 1911, subsequent amendments passed in the British version of the Act were not incorporated in the South African law, with the result that the latter remained unchanged until it was repealed and replaced in 1956 (Mathews, 1978). The Official Secrets Act created 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; making a sketch, plan, model or note which might be or was intended to be useful to an enemy; or obtaining, collecting, recording, publishing or communicating to any other person documentary or other information that might be useful to an enemy. It also prohibited the use of official information, including information about munitions of war, for the benefit of a foreign power, as well as the use of official documents for any purpose prejudicial to the safety or interests of the state (Mathews 1978).

Under a Union government, more significant than relations between white South Africans and the British government, was the exclusion of blacks from political life. Government was not accountable to this majority, which included a peasantry that was being forced off the land, a growing unskilled working class, and a politicised but small black elite (Gerhardt 1978). Each of these groups responded to their marginalisation through varying forms of protest. Collectively, the peasants who resisted their dispossession; the black workers who clashed with white miners in the urban areas, and the black elite which petitioned the overseas centres of power in protest against their political exclusion, shaped the early Union government's domestic policy. White workers were given preferential treatment including access to more skilled positions in the economy, along with the privilege of political inclusion; this was the government's dominant response to the major security issue of the time, commonly referred to as the 'Native question' (De Kiewiet 1941).

During the early Union period, foreign policy issues were rarely debated in parliament, and decisions were often taken at the executive level. Nonetheless, 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 did not have an independent international status, as the British government handled the foreign relations of its dominions directly. The 1926 Balfour Declaration defined the relationship between Britain and its dominions as one between autonomous communities within the British Empire which were 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 accompanied by the establishment of security institutions that unified the former components of the various colonies and Boer Republics. The Union Defence Force (UDF) and South African Police (SAP), both formed shortly after Union, faced the task of integrating disparate security cultures. Seegers (1996) notes that through these institutions the system of secrecy developed at an early stage. Both the Botha and Smuts governments focused the attention of the SAP on Bolshevik elements in the trade unions. Correspondingly, between 1910 and 1920 the British police focused their attention on the activities of the British Communist Party and leftists in the labour movement. London and Pretoria shared information supplied by their respective informers. Seegers also notes an early reliance on 'black detectives, informers, and trackers in stock theft cases, who were praised for their zeal' (1996:51).

The period between the two world wars saw the development of various informal institutions aimed at consolidating the position of Afrikaners in South African society. The formation in 1918 of the Broederbond, a secret organisation aimed at advancing Afrikaner interests and Nationalism, was one such initiative. In the 1940s, Nazi supporters in South Africa formed the Ossewa Brandwag (OB). Several right-wing nationalists were later recruited into the first formal civilian intelligence organisation, the Bureau for State Security (BOSS), established under Prime Minister B J Vorster, who himself had been interned during the war (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 respond to a significant show of pro-Nazism in the territory of South West Africa, at the time a South African mandate.

Encroaching on personal liberties was an integral way of the Union's machinery of secrecy and state security. Mathews (1971) notes that the Indemnity and Special Tribunal Act of 1915 provided for detention and imprisonment during World War One, and that the War Measures Act contained similar sanctions during World War Two. Both these measures were withdrawn after these wars ended; however, Mathews records,

> 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 (1971: 131).

Mathews cites two judgments concerning the Official Secrets Act during World War Two, which is the context in which the law was most extensively applied. In one case (*R v Wentzel)*, the accused (Wentzel) was charged with having prepared for postage, information that might have assisted a foreign power that was hostile to South Africa. At that time, South Africa was at war with the Nazi alliance. Wentzel defended himself by saying he had not intended to post the information, but had held it in reserve should the need arise to explain himself as a German national to a future Nazi government, which seemed probable at the time. Significantly, he was acquitted on the grounds that the state had failed to prove his intention to communicate the contents of the letter to the enemy, which was a requirement of the Official Secrets Act (Mathews 1978).

In another case*,* (*R v Vorster) the accused (*Vorster) was convicted of collecting information about the munitions and personnel at the naval base in Simonstown. In this case, the appeal court accepted that, because the information had been obtained from a person not authorised to communicate it, the accused could be assumed to have obtained the information for reasons that were harmful to the interests of the state (Mathews 1978).

The classification of records or information was of no consequence in decisions relating to whether a crime had been committed under the Official Secrets Act. Classification was merely an administrative procedure applied by government departments. A person could be prosecuted under the Act even if the information disclosed was unclassified. This was the subject of review in the United Kingdom in 1957. A committee looking into administrative procedures and tribunals – the Franks Committee – raised concerns about the classification system in place at the time. This system essentially rated documents according to the harm that could result from their unauthorised disclosure, as follows: Top Secret (exceptionally grave damage to the nation); Secret (serious injury to the interests of the nation); Confidential (prejudicial to the interests of the nation); and Restricted (undesirable in the interests of the nation (Mathews 1978:117).

The Franks Committee questioned whether these criteria were being applied in a reasonable and consistent manner, and raised concern about the fact that classification decisions were not subject to review. Moreover, the onus was placed on

a recipient of classified information to destroy it, rather than to seek a review of its classification status. This led to concerns by historians that documents were being tampered with before being made available when the time came for public release after the 30 year period stipulated in the Public Records Act (ibid).

As early as 1957, the Franks Committee made the case for a revision of the classification system in the United Kingdom. One of the recommendations was to link the system of classification with the criminal law. South Africa at the time was sinking further and further into racial exclusion and political suppression. By 1957, the NP government had all but institutionalised secrecy.

Extensive secrecy measures had been put in place in the period 1910–1945, with the Official Secrets Act of 1911 as the main vehicle. Their use by the state was driven by three key domestic and international imperatives: addressing the 'Native question', controlling the growth of the labour movement, and assisting the Allies in the war. The institutions that developed out of this effort had some of the hallmarks of modern security organisations, but these were overshadowed by the factor of racial exclusivity, which became more pronounced after the NP's ascent to power (Grundy 1986; Cawthra 1986). The British approach – particularly the promulgation and use of the Official Secrets Act – was particularly influential in shaping security and intelligence policy. It was a primary tool in the Union government's responses to various threats to its perceived interests. One major perceived threat was black resistance, a factor that shaped domestic security policy as well as the role and orientation of the security forces.

FROM 1945 TO 1960

The period after World War Two was marked by a heightened standoff between East and West, in the form of the Cold War. In line with global trends, intelligence services became a more dominant feature of South African politics. The Security Branch of the SAP was established in 1947. Drawn from the SAP's detective service, it acted as an elite political police. Domestically, it was primarily engaged in tactical intelligence; it gathered information about opponents of apartheid, and pursued short- and medium-term objectives such as detentions, prosecutions, and imprisonment.

South Africa's foreign relations in this period were a response to its growing isolation, and had to be conducted in an increasingly stealthy manner. Gone was the international stature and prominence that General J C Smuts had achieved during his tenure as prime minister, a position that saw him serve as a member of the British War Council. Information officers posted abroad were tasked with

countering 'hostile propaganda' (Geldenhuys 1984). The number of information offices multiplied, and an expanded South African Information Service was established in 1957, tasked with winning foreign support for South Africa's domestic and foreign policies. The United States, Britain, and Western Europe were singled out as priority areas. Africa was not, and the NP government maintained only one office in the 'north' – in Salisbury in Southern Rhodesia (Geldenhuys 1984).

Following its ascent to power, the NP government introduced policies aimed at enforcing racial separation and white privilege in all walks of life (Grundy 1986; Bindman 1988; Van Diepen 1988). Strong measures were required to secure the continued compliance of an increasingly defiant black population, and the period after 1948 saw the establishment of strengthened security services and the introduction of a plethora of laws designed to enforce apartheid (Bindman 1988). Besides legislation explicitly aimed at countering political resistance – commonly labelled as 'communism' – many other areas of public life were subjected to growing secrecy. Among others, the Wage Act of 1957, the Industrial Conciliation Act of 1956, the Bantu Labour Relations Act of 1953, and the Reserve Bank Act of 1944 contained severe restrictions on the public disclosure of certain types of information (Mathews 1971).

Laws aimed at suppressing freedom of expression and political association included the Suppression of Communism Act of 1950; the Internal Security Act of 1950; the Public Safety Act of 1953; the Riotous Assemblies Act of 1956; the Defence Act of 1957); and the Police Act of 1958. They were introduced in a context 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 collaboration between different racial and ethnic groups. In the Cold War context, the NP regime labelled almost all resistance to white rule as 'communist', and the barrage of legislation passed in the early 1950s was based on this assumption.

Mathews (1971) has compared South Africa with other countries that placed restrictions on political association and access to information in the early part of the 20th century. In 1917 the United States introduced its Espionage Statutes, aimed at defining the crime of espionage as the communication of documentary or other information relating to national defence to a foreign nation or agent. The United States was also one of few western democracies with extensive anti-communist laws, which encroached upon basic freedoms of expression and information as well as personal privacy and liberty.

There, the Smith Act of 1940 was introduced to counter the activities of Nazi and Fascist groups; however, it was used extensively against communists.

Other legislation included the Subversive Activities Control Act and Internal Security Act of 1950, and the Communist Control Act of 1954. Mathews (1971) notes that, unlike its South African variants, the American legislation did not enjoy free passage, and had to be refashioned to accord with the rule of law and requirements of due process. In South Africa, however, semi-authoritarian rule allowed the free passage of laws that routinely restricted information, and undermined personal liberties.

Among other things, South African legislation in this period continued to emphasise the suppression of information, rather than public access. Even 'white' institutions – including parliament and the media – were subjected to growing restrictions. The Defence Act of 1957 prohibited the publication of three classes of information without ministerial authority, thus effectively depriving the public of the right to virtually all information connected with defence, and 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 about the composition, movements, or disposition of the South African or foreign armed forces or their armaments;
- statements, comments or rumours about a member or activity of the South African or foreign armed forces calculated to prejudice or embarrass the government or to alarm or depress members of the public; and
- secret or confidential information relating to the defence of the Republic.

This last category had far-reaching implications; 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 authorised the state president to ban a publication containing information calculated to achieve the objectives of communism, or endanger the security of the state or the maintenance of public order.

The Prisons Act of 1959 made it a crime to sketch or photograph 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 used for official purposes. Effectively, this Act placed restrictions on making known the poor conditions under which prisoners might be kept. Significantly, it was introduced after the 'Treason Trial' of 1956 involving Nelson Mandela and other anti-apartheid

activists. Their photographs – and their cause – were widely publicised, which no doubt spurred this latest form of censorship.

FROM 1960 TO 1976

Growing resistance to apartheid led to intensified repression. In 1961 the ANC was banned, and its remaining leaders went into exile (Davidson et al 1976). In response to the radicalisation of liberation politics, the government experimented with different models of intelligence coordination. In 1963 it established a State Security Committee and a Working Committee (National Intelligence Service 1994). Both however, were part-time structures, and therefore largely ineffective. One reason was that the State Security Committee did not meet regularly. In 1966 intelligence co-ordination was again reviewed and the then prime minister, Dr H F Verwoerd, decided that the State Security Committee should be substituted by a State Security Advisory Council (SSAC). The latter had a secretariat, known as the Intelligence Co-ordination Division (ICD). Except for its director, the ICD consisted of non-permanent members who depended on full-time officials for basic intelligence.

In the late 1960s the cabinet felt it needed to be better informed on security issues, and the prime minister, B J Vorster, tasked a high-ranking police officer and close confidante, General H J van den Bergh, with establishing a new intelligence organisation. Initially, it was envisaged that Van Den Bergh would control the Security Police and Defence Force Intelligence. However, he advised against this conflation and an inquiry into the matter was held. The departmental intelligence services were not enthusiastic about a central intelligence organisation as they feared it would encroach on their mandates (National Intelligence Service 1994).

In September 1969 the government appointed Appeal Court Judge H J Potgieter to explore the future positioning of the intelligence departments. Completed in August 1970, his report 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 them. The government accepted this recommendation, and formed the Bureau for State Security, or BOSS (National Intelligence Service 1994; Grundy 1986).

The functions of BOSS 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; prepare and interpret for the State Security Council a national intelligence estimate concerning the security

of the Republic; formulate, for approval by the Council, policy relating to national security intelligence; co-ordinate the flow of intelligence among different government departments; and 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 government introduced the Security Services Special Account Act of 1969, which enabled it to create an account to control and utilise funds for confidential services and expenses connected with the Bureau. BOSS soon became known for its heavy-handed and intimidatory activities. Even though it did not have powers of arrest, its crude and heavy-handed tactics – harassment of journalists and editors, blatant surveillance of political meetings, tapping of telephones, and opening of mail of opponents of apartheid – quickly made it notorious (Magubane 2004).

BOSS operated domestically as well as abroad. Geldenhuys (1984) observes that intelligence services operating secretly are often very influential, and this soon happened in the case of the Bureau, which came to play a significant role in foreign relations. General Van Den Bergh, as head of the Bureau was particularly active in southern Africa as an emissary of Vorster in the détente era of the 1970s; for example, he helped to organise the historic Victoria Falls summit between Vorster and President Kenneth Kaunda of Zambia in August 1975. Former BOSS officials have stated that much of their operational effort was aimed at ending South Africa's international isolation. NIS operatives were deployed to this end both inside the country and abroad (NIS 1994).

Besides the Bureau, the other members of the statutory intelligence community and the state's secrecy system in this period were the Security Branch of the SAP, and the Division of Military Intelligence (DMI) of the South African Defence Force (SADF). Both were involved in political conflict. In the 1970s worker and community resistance to apartheid intensified, resulting in intensified repression by the security forces. The Security Branch was tasked with monitoring political resistance, and did so by co-ordinating an extensive network of informers as well as utilising draconian measures such as detention without trial, and the harassment and surveillance of opponents of the state. The Branch kept files on many anti-apartheid figures (Brogden & Shearing 1993).

The most striking feature of the DMI was the extent to which it engaged in attacks on anti-apartheid activists, many of whom were in exile, in banned political organisations such as the ANC and PAC, Umkhonto we Sizwe and Poqo (the armed wings of these two movements), and the SACP. This clearly deviated from

the conventional role of a defence force, namely to defend a country against foreign aggressors. In South Africa's case the 'enemy' was the so-called frontline states, or independent southern African states bordering on South Africa, which had to bear a threefold burden: economic domination by South Africa; the sponsorship of counterrevolutionary movements by Pretoria, notably Renamo in Mozambique and Unita in Angola; and regular strikes on ANC bases on their own soil, often at the cost of civilian lives (Davidson et al 1976; Cawthra 1986).

Besides the Defence Act, other security legislation also restricted access to information. Much information about the defence force was blacked out, thus even preventing the media from reporting on events of public interest. Thus the South African media were unable to report on SADF incursions into neighbouring territories such as Angola (Mathews 1978).

The Atomic Energy Act of 1967 criminalised the disclosure or unauthorised publication of information relating to source or nuclear materials, or research, inventions, or discoveries related to nuclear or atomic energy. The receipt of such information was also a crime. The Nuclear Installation Act of 1963 and regulations under the Uranium Enrichment Act of 1970 contained similar provisions. Again, these provisions were as broad, if not broader, than those in 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).

Access to state records by members of the public, including researchers and the media, was strictly regulated. The Archives Act of 1962 gave the director of the State Archives significant powers to manage official records. Among other things, 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 their ultimate disposal (interview with Dr Graham Dominy, 2 September 2003).

In terms of the Act, state records could only be made available to the public after 50 years. 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.

However, several departments made use of ambiguous formulations in the law to avoid its disposal requirements (TRC 1998).

Censorship of the media also played a significant role in restricting access to information. The Publications Act of 1974 prohibited the distribution, publication, or exhibition of 'undesirable' publications, films and entertainment, and enabled a committee to exercise its judgment about which media fell within the scope of acceptable norms. The committee's decisions were binding in criminal cases. According to the Act, material was deemed undesirable if it was 'prejudicial to the safety of the State, the general welfare or the peace and good order' (Mathews 1978: 151). In 1976 the Act was invoked to ban a Christian Institute publication entitled *South Africa – A Police State?* because it listed people detained under various security laws, described major political trials during the previous three years, and outlined types of torture used by the police.

Apartheid legislation also infringed on personal liberties and privacy. Section 118A, inserted in the Post Office Act in 1972, allowed mail and telephone calls to be intercepted if deemed to be in the interests of the security of the Republic (Mathews 1971).

FROM 1976 TO 1990

In 1976, following the Soweto uprising against the introduction of Afrikaans as a medium of instruction in black schools, hundreds of youths left the country to take up arms against the apartheid government. The unprecedented political resistance, and South Africa's consequent increasing international isolation, led its rulers to review their security strategy. According to the 1977 White Paper on Defence, the role of the defence establishment was 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 for maintaining white domination. The TBVC states – the 'independent' Republics of Transkei, Venda, Bophuthatswana and Ciskei – had powers to legislate on certain areas of service delivery, thus giving rise to a myth of political independence (Bindman 1988). In reality they were economically entirely dependent on South Africa; and the international community, including multilateral bodies such as the UN and the OAU, regarded them as extensions of the apartheid order. Besides these, Pretoria created several other self-governing national territories, or 'homelands', which were rejected by the majority, and internationally unrecognised (Bindman 1988). In terms of the Self-Governing Territories Act of 1971, their

governing authorities could make laws about policing, but not about intelligence. All six territories chose to establish their own police forces.

The Transkei Intelligence Service, the Bophuthatswana National Intelligence Service, and the Venda National Intelligence Service were modelled – in law at least – on the apartheid government's National Intelligence Service, but staffed by their own 'citizens'. Like the mainstream services, the TBVC services focused on frustrating their political opponents. They received training and resources from the South African government, and served the same ends, namely to prevent the country from falling into the hands of the disenfranchised majority. In addition, the police forces of all these homelands were extensions of the repressive machinery of the apartheid state. For example, while KwaZulu never developed a statutory intelligence service, its police colluded with warlords, certain chiefs, and vigilante groups to quell political opposition to its chief minister, Dr Mangosuthu Buthelezi.

The Defence White Paper of 1977 introduced the notion of a 'total strategy' to counter a 'total onslaught' on the South African social order. All aspects of national life – military, economic, political, sociological, technological, ideological, psychological and cultural – were to be co-ordinated to this end (Hansson 1990). In the 1970s and 1980s South African society became increasingly militarised. Among the more notorious security institutions was the Civil Cooperation Bureau (CCB), an offshoot of the Special Forces, which engaged in an extensive political assassination campaign (Cawthra 1986). At the height of apartheid in this period, security policy and strategy were co-ordinated by the State Security Council (SSC), a cabinet committee chaired by the state president and largely comprising ministers responsible for the country's security services.

Significantly, the heads of the intelligence services also served on the SSC, giving them great influence in national decision-making. The SCC was established under the Security Intelligence and State Security Council Act of 1972. Influential in national politics to the extent that the cabinet merely served to rubber-stamp its decisions, 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 a revolutionary strategy and principles and applied them in reverse. The NSMS continued to evolve new forms of control to counter growing national resistance and the failure of government reforms. By the middle of the 1980s state strategists began to describe South Africa as being involved in a 'war of low intensity',

requiring the mobilisation of the entire population, including black people at the grass roots (Hansson 1990; Haysom 1992).

Seegers (1996:25) describes the contest for influence and control by elements of the security forces in the mid-1980s as follows:

> 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 passed during this time. The Secret Services Account Act of 1978 provided for the establishment of an account for secret services. The minister of finance could transfer funds to the following accounts, at the request of the ministers concerned: a Foreign Affairs Special Account established by the Foreign Affairs Special Account Act of 1967; the Security Services Special Account; the Special Defence Account, established by the Defence Special Account Act of 1974; the Information Service of South Africa Special Account, established by the Information Service of South Africa Special Account Act of 1979; and the South African Police Special Account, established by the South African Police Special Account Act of 1985.

The effect of this legislation was to tighten control over information, and further restrict opposition to government policies. Moreover, the legislation was generally intrusive, giving the state an inordinate degree of control over people's lives.

The Protection of Information Act of 1982 superseded the Official Secrets Act of 1956, the Official Secrets Amendment Act of 1956, section 27C of the Police Act of 1958, sections 10, 11 and 12 of the General Law Amendment Act, 1969, and section 10 of the General Law Amendment Act, 1972. It strongly resembled its primary precursor, the Official Secrets Act, 1956 and prohibited the disclosure of certain information. More specifically, it proscribed obtaining secret state records information and disclosing such information to any foreign state or its agent. Secret information was defined as 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; and any other matter or article which might be of use to a foreign state or

hostile organisation (Protection of Information Act 1982). It placed a heavy onus on individuals to identify matters that might prejudice the interests of the state.

The Act was clearly designed to deny access to information both to foreign states and to opponents of apartheid. The emphasis was on denying 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 of 2000 as well as the National Archives Act of 1996.

Like the Official Secrets Act, the Protection of Information had no formal relationship with prevailing systems of classification. In 1978 the cabinet introduced a set of guidelines aimed at ensuring uniform standards for the handling of classified information by public servants. Commissioner Tertius Geldenhuys, head of Legal Services in the SAPS, described the background to the introduction of these guidelines. Prior to this the Official Secrets Act was in place, but there were no government regulations to standardise 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 provided for information to be classified under different levels of secrecy, as well as procedures for their handling and safekeeping (interview with Dr Tertius Geldenhuys, 7 October 2003).

In summary, it can be argued that all the components of the statutory intelligence community – NIS and its predecessor, BOSS; the Security Branch; Military Intelligence; and the intelligence services of the TBVC states – collaborated to ensure the maintenance of apartheid. This is not to deny that there were contradictions between these role players from time to time. At times, the rivalry among Military Intelligence, the Security Branch, and NIS was quite marked. But collectively these agencies wielded considerable power.

CONCLUSION

Before 1990 South African government was closed and secretive. Official secrecy and political exclusion combined to marginalise the country's black majority as well as opponents of the ruling governments. From 1912 onwards the country was subject to the British Official Secrets Act, which contained severe penalties for the disclosure of state secrets. Domestic foreign policy was driven by the imperative to resolve the 'Native question', which came to a head following the ascent to power of the Afrikaner-dominated NP. In subsequent years, much of the legislation aimed at consolidating white rule had the effect of silencing opposition

and suppressing basic human rights such as freedom of speech, movement, and expression. As shown in the earlier discussion of international conventions, the denial of these freedoms is tantamount to the denial of access to information in the broader sense.

The Protection of Information Act – which superseded the Official Secrets Act – reinforced a culture of penalising the disclosure of secrets. Important issues of accountability, of who defines what can be withheld as secret or confidential, and which checks and balances exist over how officials manage information, continued to be ignored. This is not surprising, given that apartheid South Africa was facing an unprecedented crisis at that time.

The role of the State Archives Service in managing security records appears to have been ambiguous, creating a situation seemingly exploited by the security services. Many documents were destroyed in the early 1990s, eradicating a large part of South Africa's official memory.

In the period reviewed in this chapter, the security policies and secrecy measures of successive white minority governments were aimed at consolidating white rule, while influencing international opinion in favour of South Africa's domestic policies. In the apartheid era, South Africa had neither a specific system for declassifying security-sensitive information, nor a regime of access to information. In reporting on and assessing the implications of the destruction of records, the Truth and Reconciliation Commission points out that the main guideline to public access to state records under apartheid was the Archives Act of 1962, which established that access was a privilege to be granted by bureaucrats.

The apartheid inheritance included a classification system contained in the cabinet guidelines for the protection of classified information. The classifications most commonly used by officials were 'Top Secret', 'Secret', 'Confidential', and 'Restricted'. These were captured in a cabinet document entitled Minimum Information Security Standards (MISS), and all state departments were expected to comply with its stipulations. The guidelines do not cover the issue of which officials have the authority to classify information, how that authority is derived, and under which conditions information may be reclassified.

Secrecy in pre-1990 South Africa was pervasive; it formed an integral part of the colonial and apartheid order, and caused much suffering for many people. The transition to a new political dispensation was marked 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, and to what extent, the old patterns of secrecy have persisted.

3

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

The mid-1980s to the early 1990s was an exceptionally violent period in South African history. The UDF, a broad front of extra-parliamentary organisations, was launched in 1983 to oppose attempted government reforms, including a racially based tricameral parliament. The South African state, particularly the security forces, responded with a growing show of force and increasing repression: detentions without trial, prosecutions and imprisonment under anti-terrorism and internal security legislation, political assassinations by apartheid hit squads, and the instigation of 'black-on-black violence' (Collinge 1992).

Through most of the 1980s the P W Botha government challenged the ANC to renounce violence, while the ANC, retorting that it was the government that should do so, encouraged its followers to continue to pursue an armed struggle, mass action, and South Africa's international isolation. The government's posture changed dramatically after F W de Klerk succeeded Botha as state president in 1989, although, even under the latter, secret talks were initiated with the ANC to explore the possibility of a negotiated political settlement .

De Klerk's unbanning of the ANC, PAC, SACP, and other restricted organisations took observers as well as the liberation movements by surprise. Nelson Mandela and other high-profile political prisoners were released, and exiled leaders returned to pave the way for negotiations (Haysom 1992). In May 1990 the government and ANC signed the historic Groote Schuur Minute which expressed 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). They reaffirmed this commitment in the Pretoria Minute later that year.

In the early 1990s the government discourse around security began to change. Shortly before the unbanning of the ANC, De Klerk addressed a meeting of the country's top 500 police officers at which he impressed upon them that they had new responsibilities, and urged them to leave politics to the politicians (Nathan & Phillips 1992).

From February 1990 onwards, political parties and organisations across the political spectrum began to give urgent attention to formulating alternative policies. The ANC held a major policy conference in June 1991. Meanwhile, implementation of the Groote Schuur and Pretoria Minutes, particularly the return of exiles and the accompanying amnesty process, the release of political prisoners, and measures to contain political violence still raging across the country, proceeded with difficulty. The main parties made accusations and counter-accusations about the real intentions of their counterparts. By this stage some 10 000 people had lost their lives in political violence since 1986, and more than 30 000 had been displaced (Haysom 1992). Levels of public confidence in the ability of the security forces to contain the violence were very low, and in April 1991 the ANC threatened to suspend negotiations. The stop-start process continued for several months, but the government and other parties finally agreed on multiparty talks to discuss an inclusive political dispensation. This resulted in the Conference for a Democratic South Africa, or CODESA (Friedman 1993).

CODESA's first meeting, held in December 1991, provided a platform for the various parties to express their intention to negotiate a political settlement. But most of the work was done in five working groups, dealing with a climate for free political activity; constitutional principles to be included in a new constitution, and a constitution-making forum; transitional arrangements; the future of the TBVC states; and time frames and modes of implementation (Haysom 1992). While initially unhappy about this proposal, the government eventually agreed that decisions taken at CODESA would be binding. The parties also agreed that decisions would be taken on the basis of 'sufficient consensus' among participants. This effectively meant that the government and the ANC would have to agree if the process was to move forward.

Discussions in the working groups continued over the next year, and CODESA 2 convened in May 1992 to consider the results. However, the CODESA process broke down because important issues relating to the constitution-making process had not been resolved. The government and ANC began talks aimed at getting the negotiations back on track.

The volatile political climate did not lend itself to the resolution of differences, but by this stage both the government and the ANC realised that they were so deeply embroiled in the process that they dared not let it fail (Friedman 1993). In September 1992 they signed a Record of Understanding which dealt with a number of outstanding issues.

While negotiations continued, with a broad range of opposition organisations rallying behind the ANC, citizens made limited inputs. The ANC tried to broaden participation by holding consultative meetings with other organisations, including its alliance partners, the SACP and Congress of South African Trade Unions (COSATU), and holding public meetings, but policy and strategy were largely determined by its leaders. Similarly, in February 1992 the government called a referendum to seek endorsement for the adoption of an interim constitution (Friedman 1993).

THE MANAGEMENT OF INTELLIGENCE INFORMATION DURING THE NEGOTIATIONS

The transition to a new intelligence dispensation formed part of a broader process of political accommodation that stemmed from the work of Working Group One at CODESA. Working Group One dealt with the creation of a climate for free and fair political activity, and it split up further into three sub-working groups dealing with 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). In its final report it recommended that the security forces be subject to the constitution; politically non-partisan; respect human rights, non-racialism and democracy; and strive to be representative of the society as a whole. Working Group Three agreed that the security forces should be controlled by the interim government.

At this time, the 1983 tricameral constitution was still in force. While it did not create a right of access to information, politics were being liberalised, enabling the media to report more freely on significant national events. However, security legislation such as the Internal Security Act, the Riotous Assemblies Act and the Terrorism Act remained in place. Intelligence services were managed as separate entities, and the intelligence information of the state was firmly under lock and key in state hands, unauthorised access to it being a criminal offence.

Intelligence services played a significant role in the negotiations, and representatives of services on both sides were drawn into the process to map out a new intelligence dispensation (O'Brien 1996). The ANC's Department of Intelligence

and Security (DIS) had been formed in 1969, to counter attempts by the South African state to crush Umkhonto we Sizwe.

In 1992, Joe Nhlanhla, the ANC's head of intelligence, wrote that the apartheid security services were pervaded by a militaristic and racist ethos, served the interests of the NP regime rather than those of the people, and were steeped in a culture of secrecy and lack of transparency and accountability. Because of this, they were able to resort to detention and torture, assassinations, and kidnappings. This was an inward-focused approach where the greatest threat to national security was seen to come from fellow South Africans. However, he said intelligence services did have a role to play in the affairs of state, and added that

> the world over, intelligence activity is, by its very nature, characterised 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 (1992:70).

NIS claimed it had played a constructive role during its existence, which was roughly as long as that of DIS. Daniel Barnard, a former head of NIS, said during his term of office it had not only supplied intelligence, but had also facilitated negotiations between the apartheid government and its opponents. He said NIS had been able to play this role because it was 'schooled in the age-old universal fundamentals of the intelligence profession: it seeks the truth, and undauntedly conveys it to the government' (National Intelligence Service 1994).

In 1992 the new director-general of NIS, Mike Louw, spoke of the need for greater openness in intelligence matters, and promised that the agency would become more transparent (*Sunday Times*, 23 February 1992). Under President De Klerk, control over the intelligence services was shifted from the State President's office to the minister of justice.

The ANC's framework for security policy was very similar to those of liberal democracies in the post-Cold War era. It adopted the following resolution at its June 1991 policy conference, which became the basis for its input into the negotiation 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 (ANC 1991).

According to senior ANC members, the NP government initially resisted the idea of negotiating a new intelligence dispensation, on the grounds that intelligence issues could not be discussed in open political forums. It offered to simply absorb members of the intelligence services of the liberation movements and TBVC states into NIS. The ANC rejected this proposal, and the political players, including representatives of the various intelligence services, went on to negotiate a new intelligence dispensation (interview with Moe Shaik, 17 October 2003).

DIS and NIS were determined not to allow setbacks in the political negotiations to derail their efforts to find common ground. They held a series of bilateral meetings, resulting in agreements on a set of basic principles for intelligence work in the new dispensation, the need for the establishment of a subcouncil on intelligence under the authority of the impending Transitional Executive Council, and the terms of reference of such a subcouncil.

It was during this early period of the transition that huge quantities of apartheid security records were apparently destroyed. The previous chapter has already examined the implications of the state's view that 'sensitive records' fell outside the ambit of the Archives Act. In 1992 the ANC Commission on Museums, Monuments and Heraldry proposed a moratorium on the destruction of state records, but was powerless to see this through (interview with Verne Harris, 1 September 2003). Instead, the cabinet authorised various government departments to destroy sensitive records.

The devastating consequences of this decision was recorded by the country's Truth and Reconciliation Commission, established by a 1995 act of parliament. In a six to eight month period in 1993, NIS alone destroyed about 44 tons of documents and microfilm – all official records. All state departments were instructed to transfer documents that had originated as State Security Council Secretariat records to NIS, which at the time provided secretariat services to the State

Security Council. Among other destruction facilities, the furnaces of the Iron and Steel Corporation (ISCOR) plant in Pretoria were used for this massive incineration exercise. According to the TRC, much of the destruction took place outside the parameters of the guidelines for the disposal of records, and was intended to obliterate all information about operations, sources, or other compromising information that the security establishment might have to explain in the future. This created a massive vacuum in the corporate memory of NIS as well as other security institutions (TRC 1998).

The ANC and other liberation movements were probably unaware of the extent of the destruction of records in this early period, and powerless to prevent it in any case. The government had only just lifted its restrictions on the movement, which, together with extraparliamentary organisations, had been intensely scrutinised by state security forces and intelligence services. The fact that the two sides were engaged in 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 TEC

The status, legitimacy, and ownership of intelligence information in the course of the transition to democracy is central to our enquiry. This was undoubtedly an area of contestation. An analysis of policy, legislative and administrative instruments established or enforced in that period suggests an ambiguous impact on access to and control over information generated by the apartheid-era security institutions.

The Transitional Executive Council Act of 1993 gave expression to the arrangements agreed to in the negotiation process. While democratic elections were being prepared, the country would be jointly governed by the NP and major entities. Seven subcouncils – on defence, law and order, intelligence, finance, the status of women, foreign affairs, and regional and local government – were set up to facilitate this process. Their role amounted to a form of multiparty scrutiny over these areas of governance. The role of the subcouncil on intelligence, as prescribed by the act, was to devise basic principles for intelligence work which could also anchor a new democratic dispensation. It was also tasked with formulating a code of conduct that would bind all services during the transitional period, and foreshadow a code in a democratic South Africa (TEC Act 1993).

Under the TEC, the intelligence services of the NP government, the TBVC states and the liberation movements would remain intact. They would continue to provide their principals with information during this vital period, but were expected

to start crafting a unified intelligence framework. Unavoidably, the leaders of these intelligence institutions were drawn into negotiating their common future.

The TEC Act also provided for the establishment of a Joint Coordinating Intelligence Committee (JCIC), tasked with providing the TEC with estimates of the security situation in the run-up to the elections. The ANC initially wanted all intelligence structures to report to the JCIC, but backed down when NIS insisted that all the services should retain control of their day-to-day activities. The JCIC comprised the heads of all the civilian, police, and military intelligence services, and effectively managed them during this period of transition. Besides providing the TEC with intelligence, the JCIC played a vital role in the run-up to the election by ensuring that all factors that could derail the process were monitored (interview with Moe Shaik, 17 October 2003).

After completing its task, the JCIC – following a recommendation of the subcouncil – established a forum called the Heads of Civilian Services (HOCS), comprising the heads of the various civilian intelligence agencies, and a provisional national intelligence co-ordinating committee. The task of HOCS was to continue developing proposals for a future intelligence dispensation, begun under the auspices of the subcouncil. The task of the coordinating structure was to ensure that the joint intelligence process continued beyond the legal mandate of the TEC.

While NIS and DIS co-operated to some degree, they were still on opposite sides of the political divide in this critical period. Despite the formal co-operation introduced by the establishment of the TEC, secret information was a contested area. Both the NP government and its political adversaries, particularly the ANC, were aware of the huge influence of intelligence agencies in this sensitive period, and kept up their intelligence offensives in order to learn as much as possible about the other side. The existence of a legislative regime that criminalised the disclosure of information, internal regulations that bound members of the security services to secrecy, and the absence of records make it almost impossible to assess objectively the role of NIS at that time.

The wide-ranging Protection of Information Act, 1982 and other draconian security laws such as the Internal Security Act remained in force, even as the opposing political forces engaged each other. A double-edged sword, security legislation was probably as much directed at the liberation movement, with which the government was busy negotiating a new political dispensation, as the white right wing, which was engaged in violent attempts to derail the talks. The volatility of the situation should not be underestimated. There were major divisions in the apartheid security forces, with a number of members aligned with

the extra-parliamentary white right wing. The government and others feared that security information might be leaked to the right wing, and a climate of mutual fear and distrust pervaded the ranks of the security forces (Haysom 1992).

A key issue was the status of intelligence records vis-à-vis the state archives. According to the TRC (1998), the 1978 cabinet guidelines on the protection of information empowered the heads of government departments to authorise the destruction of state records. In the process, the guidelines ignored the provisions of the Archives Act, which gave final custodianship of all state records to the State Archives. The guidelines did not explicitly state that the powers given to the director of the State Archives were being replaced or retracted. But the weight of a cabinet decision was sufficient to allow government departments to act without hindrance in destroying state records. This power was exercised routinely within the security establishment. The State Archives Service claimed it only became aware of the guidelines during 1991.

From 1983 the routine destruction of records was commonplace in NIS, which assumed that its records fell outside the ambit of the Archives Act. Marius Ackerman, former state law advisor in the State President's Office, in describing the status of official documents in the custody of NIS, 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).

In testimony before the TRC, former NIS officials admitted that the organisation had destroyed about 44 tons of records in the months preceding the first democratic elections. Thousands of officials in the security services and other government departments shredded and burnt all records that could give the ANC-led government insight into the methods, informants, and operations of the apartheid intelligence agencies. The TRC notes, however, that records which could not be traced included those of the National Security Management System (NSMS), a substructure of the State Security Council (TRC 1998). President F W de Klerk disbanded the NSMS in 1989, and reduced the status of the SSC to that of an ordinary cabinet committee (Hansson 1990). This was done at a time of growing popular and international resistance to apartheid, as well as growing schisms within the ruling party.

Following the mass destruction of records, apparently driven by the above-mentioned interpretation, it would seem that few records of NIS activities under apartheid survive. This institutional memory is unlikely to be recovered. The apartheid real workings of the NIS thus remained a secret, despite the occasional public relations exercise such as media interviews.

THE MANAGEMENT OF INTELLIGENCE INFORMATION UNDER THE INTERIM CONSTITUTION

Despite ongoing political violence, agreement was eventually reached on a new interim constitution. It came into effect on 27 April 1994, the day of the country's first inclusive elections. It contained an entirely new feature in South African politics: a bill of rights, which guaranteed a range of fundamental rights including the right to life; equality before the law; privacy; freedom of expression, association, and movement access to the courts; administrative justice; and, most significantly, access to information (Mureinik 1994).

On the last-named right, the interim 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).

In the period after the elections the intelligence services struggled to come to terms with their identity as defenders of the new political order, crafted by the country's first fully democratic legislature, and the broadened concept of security contained in the interim constitution was undermined in practice by discontinuities in both the discourse and practice of security. Notably, they continued to destroy records until 1996 when the cabinet finally declared a moratorium on this practice (TRC 1998).

Following the transition to democracy, intelligence officials were given wide discretion to classify information generated in the course of their work. The practice within the security services was to shield from the public view even those categories of information that would cause no harm if they were disclosed. The ANC continued to keep secret files on the activities of key government figures (interview with Moe Shaik, 17 October 2003).

Without a reasonable degree of transparency, members of the public would obviously be at a loss as to what information they might request from the intelligence services. Within the statutory services – 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 their disclosure would cause. The criteria for classifying information were also not subject to any scrutiny, because no oversight framework existed for doing so.

By April 1994 the statutory and non-statutory intelligence institutions were already locked in intensive discussions about their integration. After the elections, flowing from the reports of the Subcouncil on Intelligence, further bilateral talks were held to develop a future intelligence dispensation. These discussions influenced the debate within the new parliament. A White Paper on Intelligence and three Bills, namely the Intelligence Services Bill, National Strategic Intelligence Bill, and 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 signalled 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 (White Paper on Intelligence, 1994).

The White Paper dealt with safeguarding the country's democratic constitution; upholding the individual rights enunciated in the Bill of Rights; promoting the interrelated elements of security, stability, co-operation and development, both within South Africa and in relation to Southern Africa; contributing to global peace; promoting South Africa's ability to face foreign threats and enhance its competitiveness (Africa & Mlombile 2001).

The intelligence services would be governed by the following principles, all in sharp contrast with those 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 proposed the amalgamation of the statutory and non-statutory intelligence services into two civilian intelligence departments: the SASS, a foreign department responsible for collecting information about external threats to security; and the NIA, a domestic department focusing on internal threats. NIA would also hold the counterintelligence mandate, and ensure that foreign agents did not penetrate the South African intelligence machinery (Africa 1994).

The National Strategic Intelligence Bill provided for a mechanism to co-ordinate and integrate the intelligence inputs of the two civilian departments with those of the SAPS and SANDF, in order to advise the government on threats and potential threats to the security of the country and its citizens.

Thirdly, the Committee of Members of Parliament on and Inspector-Generals of Intelligence Bill provided for a multiparty parliamentary oversight committee able to receive reports, make recommendations, order investigations, and conduct hearings on matters relating to intelligence and national security; and an Inspector-General tasked with investigating complaints about the intelligence services. The committee would also submit reports to parliament on the performance of its duties and functions.

On the basis of cabinet recommendations, the minister of justice presented the three bills to parliament. Members of HOCS and their legal advisors appeared before the select committees of the national assembly and senate. After much deliberation and debate, the select committees recommended that the bills be tabled in parliament (interview with Moe Shaik, 17 October 2003).

Anticipating the new legislation, HOCS instructed various subcommittees to start work on amalgamating the various intelligence services. Joint special work groups were established to made recommendations in respect of the structures, budget, assets, and human resources policies of the new services. Based on their reports and recommendations, HOCS formed an Amalgamation Committee (AC) tasked with co-ordinating and implementing the establishment of the NIA and SASS. The AC established a number of so-called super working groups consisting of representatives of the statutory and non-statutory intelligence services, tasked with implementing the decisions and agreements of HOCS, and focusing on the practical issues that would be encountered in the course of the transition.

They were full-time bodies, and their reports were processed by the AC for consideration by HOCS.

Some of the issues addressed by the working groups were the staff requirements of the planned intelligence agencies, practical steps towards the proposed structural changes, budgetary implications for the 1995/6 financial year, and an orientation programme for all members of NIA and SASS. The working groups also identified functions to be shared by the two services, and mechanisms to ensure that these facilities were appropriately distributed and managed.

The interim constitution did not contain any principles governing national security, as these were still being debated, and also did not refer to the establishment of the new services. Parliament passed the three bills setting up the new intelligence dispensation in the latter half of 1994, and it effectively came into being on 1 January 1995.

Changes within the intelligence structures of the SAPS were also informed by the outcome of the negotiations (Africa & Mlombile 2001). The new government's agenda on law enforcement was shaped by two objectives: rehabilitating the police force to ensure that it served the communities of South Africa rather than political ends; and mobilising citizens to participate in the achievement of safety and security (Africa & Mlombile 2001). Among the oversight mechanisms provided for in law were an Independent Complaints Directorate, tasked with receiving complaints from members of the public about police misconduct, and parliamentary oversight over the SAPS.

Rauch (1991) describes the complexities of reorienting the police, and the sometimes ambiguous signals sent out in the course of police reform. Significantly, the rank structure of the SAPS was demilitarised, and appropriately skilled civilians appointed to a Secretariat for Safety and Security, responsible for developing policy for the post-apartheid police service.

The governance and orientation of the armed forces also changed significantly in the post-apartheid period. These were the product of political negotiations about the integration of the armed wings of the liberation movements and 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 of 1995 provided for a restructured Department of Defence comprising the SADF (under the operational command of the chief of the armed forces), and a civilian Defence Secretariat, responsible for formulating policy, and headed by the Secretary for Defence (Africa & Mlombile 2001).

The final constitution later provided the context for the reform of the armed forces, and established a framework for civil–military relations appropriate to

a democracy. It defined the primary role of the defence force as defending and protecting 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, function within the ambit of the law, and subject itself to parliamentary oversight.

Defence Intelligence structures, falling under the operational command of the SANDF, and subject to the policy determined by the Department of Defence, were also subject to the National Strategic Intelligence Act of 1994. The Act distinguished between domestic and foreign military intelligence, and prescribed the process to be followed to collect domestic military intelligence by the defence force, in support of the police. The rationale for these strict controls was to bolster the professional status of the military and to avoid situations where it could become involved in domestic political conflict (Africa & Mlombile 2001).

The introduction of a statutory co-ordinating mechanism for the intelligence agencies managed by the Minister for Intelligence was another significant development, aimed at pre-empting inter-agency rivalry. In terms of the National Strategic Intelligence Act, a co-ordinator for intelligence was responsible for coordinating the supply of intelligence by the different agencies to intelligence clients. NICOC mainly consisted of the co-ordinator and the heads of the intelligence services. NICOC was required to provide strategic intelligence assessments, including an annual estimate of threats to national security which policy-makers should heed in the course of the following year.

After the 1995 transition, the intelligence services struggled to manage the shift in orientation. The political climate was still volatile, and the new government faced the task of neutralising disaffected right-wingers, some of whom had access to security resources. 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 destabilising the country – existed in the country's security forces (O'Brien 1996).

Senior appointments made to the leadership of the intelligence services, reflected the political compromises in the course of the negotiation process. The civilian intelligence services were required to report to the president, initially through a deputy minister. In practice, the deputy minister reported through the minister of justice, who was also the minister of intelligence. The first director-general of the NIA was Sizakele Sigxashe, previously a senior figure in DIS, while the first director-general of the SASS was Mike Louw, previously director-general of NIS. The minister of defence was Joe Modise, a former ANC military commander,

and the Chief of Staff Intelligence was Lieutenant-General Dirk Verbeek, a former SADF officer.

In the SAPS, Divisional Commissioner André Grové who was responsible for intelligence and who served under National Commissioner George 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 in that period were the product of political differences at the top. This affected the quality of intelligence provided to the government. One of these incidents was the hand delivery of a classified intelligence report to President Nelson Mandela by the Chief of Defence Intelligence. The report had bypassed the NICOC structures and claimed that senior military officers from 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).

According to Africa and Mlombile, the South African experience of reforming its intelligence services held some important lessons. The first was that the envisaged mission, orientation, and structures of accountability of the intelligence services should be clearly reflected in policy and in subsequent legislation. The second was that the government should respond decisively to abuse or violations of the law, as a means of propagating a new culture. The third was that internal procedures should be comprehensively reviewed to ensure that they were consistent with the legal framework. The fourth was that each service should have clear procedures for authorising operations, thus enabling the responsible minister to confirm the legality of a particular operation. Finally, parliamentary oversight bodies had a vital role to play in monitoring such a transformation.

IMPACT OF THE CONSTITUTION ON THE INTELLIGENCE SERVICES

Section 198 of the final constitution of 1996 spelt out the principles of a new security dispensation. It stated that the security services had to be structured and regulated by national legislation, and also stipulated 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 1996, section 199).

Section 210 spelled 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 member (Constitution section 210).

In chapter 9, the constitution introduced a number of constitutional instruments aimed at promoting the transparency of the state's security organs, as well as their good governance, including a Public Protector; a Human Rights Commission; a Commission for Gender Equality; an Independent Electoral Commission; an Auditor-General; and a Commission for the Promotion and Protection of the Rights of Cultural, Religious and Linguistic Communities (RSA Constitution, 1996; section 181).

Most importantly, the constitution 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 held by another person. As in the case of the interim constitution, rights in the Bill of Rights are subject to reasonable and justifiable limitation.

PARLIAMENTARY OVERSIGHT AND ACCESS TO INFORMATION

The first post-apartheid parliament faced the gargantuan task of replacing apartheid legislation with laws that reflected the promises made to the electorate, thus laying the foundation for the transformation of South African society. In respect of the intelligence services, as with much of the civil service, not only would this entail formulating new policies and creating a new legal framework, but also amalgamating six separate bureaucracies. By law, all the operatives of the six

founding agencies were to be absorbed into the three new intelligence structures: the NIA, the SASS, and the NICOC. As noted earlier, the Committee of Members of Parliament on and Inspector-Generals of Intelligence Bill, later renamed the Intelligence Services Control Act, provided for the establishment of a committee of members of parliament on intelligence as well as inspectors-general, and had the effect of placing the intelligence services under considerable oversight.

One of the ways in which parliament could exercise its oversight role in the post-apartheid period was by questioning the responsible minister. However, as Hansard shows, this method was not utilised extensively, and questions by members of opposition parties were often on very specific issues. These were often administrative, and the minister could easily provide cryptic answers. This was done usually after consulting the relevant head of department, although in the end the minister had to decide how to respond.

The process of parliamentary questions allowed members of parliament who had served in the previous government to be called to account. On 6 September 1994 Inkatha Freedom Party member V B Ndlovu asked F W de Klerk, then executive deputy president and chair of the cabinet committee on security and intelligence, the following question:

1. Whether the National Intelligence Service (NIS) was responsible for the (a) production (b) publication and/or (c) distribution of a document entitled 'Political Conflict in KwaZulu/Natal – the role of traditional leaders'; if so, (i) which branch of the NIS, (ii) what were this document's circulation figures, and (iii) what was its purpose;
2. Whether the NIS was authorised to (a) produce, (b) publish and/or (c) distribute this document; if so, by whom; if not what is the position in this regard;
3. Whether he has taken or intends taking any steps in this regard; if not, why not; if so what steps?

De Klerk's reply was frank, probably so because it no longer held major political implications. He confirmed that the NIS had been responsible for the document, but denied that it had been distributed. It had only been a working document to be considered by a provisional production unit of the intelligence community. The document had also not been distributed to the official clients on the distribution list for intelligence products, and had only been distributed to a limited number of members of the intelligence community for evaluation and comment. He added that the document was not published and distributed because there was insufficient information to substantiate the working document.

Other questions put to ministers responsible for the intelligence services over the years have covered the status and progress of disciplinary hearings, the use of consultants in the departments, the relationship of the services with certain companies, and information about the alleged misdemeanours of officials which might have become public knowledge.

Different ministers have handled questions differently over the years. Some have bluntly referred MPs to the Joint Standing Committee on Intelligence. This has also happened in cases where an MP was also a serving member of the JSCI, but asked questions in parliament. On 23 April 2001, Brigadier-General P J van Schalkwyk, a member of the opposition Democratic Party and a member of the JSCI, asked the minister for intelligence:

- Whether a permanent investigative group had been established to deal with the backlog of disciplinary cases within the NIA, and what progress had been made;
- What the NICOC, the NIA, the SASS had spent each year on salaries, operating costs, and capital costs since 1995; and
- How many people had been employed in the Ministry of Intelligence, NICOC, the NIA, and SASS in each year since 1995.

In each case the minister at the time, Lindiwe Sisulu replied: 'The honourable member is referred to the Joint Standing Committee on Intelligence for the details on this question'.

Several years later, in 2004, the newly appointed minister, Ronnie Kasrils, took the step of disclosing, during his budget vote, the total allocation to the intelligence services as well as expenditure on personnel, operations, and capital. However, in subsequent years he did not disclose the amounts, but rather the ratios of operational, personnel and capital expenditure by the services.

Another mechanism through which parliament has exercised a degree of oversight, and which has therefore afforded the public a degree of transparency about intelligence, has been the JSCI. The founding act gives the committee – whose members are vetted by the NIA – access to classified information and documents in the possession or under the control of a service, to the extent that such access is necessary for the performance of its functions, and on condition that such information and records are handled in accordance with the existing security regulations. However, the services are not obliged to disclose the names or identities of service members, sources, or methods of intelligence gathering to the committee. Moreover, committee members are required to undergo a security clearance process, managed by the NIA. The committee functions within the

bounds of secrecy of the intelligence services, and has had to maintain a fine balance between being publicly accountable, satisfying parliament that the services are operating within the framework of the law, and remaining impartial.

THE ROLE OF THE INSPECTOR-GENERAL OF INTELLIGENCE

The Intelligence Services Control Act also provided for the appointment of an Inspector-General or inspectors-general tasked with monitoring compliance of the services with their own policies, reviewing their activities, and performing all functions designated by the minister for intelligence.

The Inspector-General is nominated by the oversight committee, and has to be approved by a joint sitting of both houses of parliament with a 75 per cent majority, following which the president is required to effect the appointment.

The inspector general is a powerful figure in the intelligence dispensation and has access to all classified records, provided they are needed for him or her to perform a stipulated function. Among the reports the Inspector-General is 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.

THE ROLE OF THE AUDITOR-GENERAL

A prominent feature of the intelligence dispensation under apartheid was the extent to which laws enabled the services to be funded in secret. As noted earlier, the Security Services Special Account Act provided for the establishment of a Security Services Special Account, to be utilised for services of a confidential nature and expenses connected with BOSS deemed to be in the public interest.

Upon the request of relevant ministers, the minister of finance could transfer funds to a Foreign Affairs Special Account; a Special Defence Account; an Information Service Special Account, and a South African Police Special Account. These were to be used for confidential projects approved by the respective ministers (interview with Wallie van Heerden, 21 October 2003).

In terms of the enabling legislation, the executive was primarily responsible for secret or special projects, and parliament knew very little about them.

Annual reports of the Auditor-General provide some insight into the services' financial accountability. An office of the Auditor-General was created in the 1996 constitution, which requires this office to audit the accounts, statements, and financial management of all national, and local government institutions, and

report to any legislature with a direct interest in the findings. The constitution explicitly requires that all reports of the Auditor-General must be made public. In 1996–7 the Auditor-General reported that although the financial statements of the intelligence services were not being published for 'strategic and security reasons', they fairly reflected the financial position of the institutions concerned. Nevertheless, he commented on the need for improved controls over the payment of human sources; the failure of the civilian intelligence services to compile asset registers; a lack of financial control over the amalgamation of the security agencies of the TBVC states with the national police service and intelligence agencies; and the failure to appoint an Inspector-General (Report of the Auditor-General, 1996/7).

The same concerns were noted in the next two reports. The report for 1997/8 stated that although progress in attending to some of the concerns raised had been slow, the relationship between the Office of the Auditor-General and the respective departments was dynamic and revealed at the least a sense of accountability on the part of the services.

Concerns about financial management were not confined to the intelligence services. Many departments attracted negative audit reports in the early post-apartheid years, an indication of the legacy they were adopting as well as the lack of managerial experience of many new officials.

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 gave them more flexibility to achieve objectives, but made them criminally liable for any mismanagement of state resources. The intelligence services are fully bound to comply with the Acts's provisions that prescribe a uniform, outcomes-driven and transparent approach to financial management in the public sector.

Members of the intelligence services sometimes question whether disclosure of the intelligence budget and the processes for determining it could compromise their task of identifying threats to national security (interview with Billy Masetlha, NIA director-general, 4 August 2005). They also ask whether their adherence to the statutory and regulatory processes of public financial management could have similar unintended consequences. These questions are particularly pertinent in the context of the Promotion of Access to Information Act.

On the one hand, the PFMA attempted to ensure open and transparent budgetary processes, with a minister given clear responsibility for financial management. On the other hand, intelligence legislation allowed the services to operate in secret to execute their mandates, and required the minister to do everything in his or her power to facilitate their work.

CONCLUDING REMARKS

In order to understand 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 of people had already died in political violence. The security forces had not only failed to turn the tide, but – as subsequent investigations showed – had sometimes fomented the violence.

The principles arising out of the political negotiations as embodied in legislation creating a transitional authority, the interim and final constitutions, and the laws establishing the new intelligence dispensation created a new culture of accountability and transparency in respect of intelligence. The new services faced many challenges, but oversight bodies appeared to be satisfied with their performance during the first five years.

Even though the services operated under new laws which entirely repealed their predecessors, there were significant continuities with the old dispensation. In the HOCS phase, agreement was reached that the administrative systems of the apartheid-era NIS would initially be used and revised within a short period. In reality, the review happened very slowly and much later than anticipated, and the new services inherited and came to operate under the arcane regulations and systems of the old order.

Moreover, the constitutional right of access to information coexists uneasily with the laws and administrative instruments designed to protect classified information. These laws and instruments are vestiges of the apartheid era and include the Protection of Information Act of 1984 and the Minimum Information Security Guidelines, which empowers public officials to restrict access to information.

On the other hand, the new dispensation has many positive features. Oversight structures, such as the JSCI and Auditor-General are able to bring both the strengths and weaknesses of the intelligence services to the attention of the public. The minister is held to account in parliament, and the services are, for the first time, united about the nature of threats to national security.

While the process of restructuring the intelligence services has been fairly comprehensive, it has not been without its problems and weaknesses. Nowhere is this more evident than in the Janus-like legislative and regulatory dispensation, which simultaneously encourages disclosure and openness on the one hand, and allows the withholding of classified information on the other.

PART TWO

The new dispensation

4

MECHANISMS FACILITATING ACCESS TO INFORMATION ABOUT THE INTELLIGENCE SERVICES

In democratic South Africa, several important mechanisms facilitate access to information about the intelligence services, either directly or indirectly. This chapter reviews these mechanisms and institutions, and assesses their efficacy.

A WRITTEN POLICY FRAMEWORK

Chapter 11 of the constitution outlines the principles governing national security, including the establishment of intelligence services subject to multiparty oversight. The White Paper on Intelligence also provides a broad policy framework as well as a basis for the legislation that sets up and regulates the intelligence services: the Intelligence Services Act of 2002, the National Strategic Intelligence Act of 1994, and the Intelligence Services Oversight Act of 1994. These Acts spell out the mandates of the services, the oversight structures, and the respective duties of the various role players, including the minister, the heads of the departments, the JSCI, and the Inspector-General. The intelligence services are also subject to PAIA, which plays a pivotal new role in allowing and regulating access to state information, and will be examined in greater detail in the next chapter.

The governing principles, establishment, functions and mandate of the intelligence services are codified in law, which is essential for public access to information. The issue is how widely known and understood these laws are, and whether the general population realises their significance. In addition, many of the regulations made under these laws are classified, and are not gazetted for public comment. In 2002, after an extensive review of the conditions of service

in the intelligence services, the minister for intelligence gazetted a set of human resources regulations for public comment. However, this is not the general trend. The norm is that regulations issued by the minister and policy directives issued by the directors-general are kept confidential, without any serious evaluation of whether the information contained within warrants protection.

PARLIAMENT

Parliament, through its law-making function, is another institution that provides a window into the functioning of the intelligence services. For those interested in the issues, Hansards – records of parliamentary debates and legislative processes – are easily accessible. All tabled legislation is subject to the normal processes, and public hearings may be held when there is considerable public interest in a matter.

Parliament is also the forum in which concerns or matters of policy can be raised with the minister responsible for the intelligence services. Although, compared to other portfolios, the minister receives a relatively low volume of questions, the mechanism is nevertheless available. In some cases, the minister refers questions to the JSCI, which effectively means that the broader public is denied the answers.

Through the JSCI, parliament also has the opportunity to consider the budget of the intelligence services before the vote. Like other multiparty parliamentary committees, work is done largely in committee, and the position of the committee is reflected in the annual budget vote of the minister. The JSCI is required to publish an annual report but its performance in this regard has been rather poor. The report usually appears late, and no special effort seems to be made to distribute it to members of the public, or even to public interest bodies that want to know more about the committee's oversight work.

THE EXECUTIVE

One cabinet minister is explicitly responsible for the intelligence services and is the figure who can be asked to account for their performance or deficiencies. The minister must report on the work of the services to colleagues in cabinet. In addition, the minister must ensure that the services provide intelligence to departments and, most importantly, relevant and timely national strategic intelligence. Members of the public are not privy to this intelligence, which is usually classified secret. However, through the budget vote, the minister provides some insight into security concerns and the broad measures put in place by the services to address

them. In responding to the minister, the JSCI usually sheds some light on current concerns and potential threats. The minister also issues public statements, and responds to queries from the media about matters concerning the services.

One criticism of the executive is that it does not currently assess whether there is intelligence that no longer needs to be kept secret, and can be placed in the public domain. There is currently no legal requirement for it to do so, and the matter therefore appears to be discretionary. Several intelligence services around the world issue unclassified or declassified reports relating to national security, as a way of keeping the public informed of the intelligence services' preoccupations.

THE INSPECTOR-GENERAL FOR INTELLIGENCE

The public is meant to have access to another important role player: the Inspector-General for Intelligence. This very senior official, whose appointment has to be approved by 75 per cent of members of parliament, has unfettered access to the records of the intelligence services, irrespective of their secret status. Such access should help the Inspector-General to evaluate properly, complaints and cases brought by members of the services or members of the public. In reality, the Inspector-General's Office has limited capacity and has experienced teething problems. The office has made efforts to publicise its existence, for example through brochures and a website. In the period under review, a growing number of complaints were received both from members of the public, and from members of the services, which the office understandably dealt with in confidence. However, no public reports have been released; so, ironically, although the office is part of the transparency mechanism, members of the public cannot readily assess its performance.

THE AUDITOR-GENERAL

The Office of the Auditor-General is a constitutional body with full authority to audit the financial statements of the intelligence services and to provide a public assessment of whether they meet generally accepted accounting standards. Regulated by the Public Finance Management Act of 1999, the financial accounting of the intelligence services is subject to the same rigorous auditing standards as any other government department. Over the years, a smoother working relationship has developed between members of the services and members of the Auditor-General's office who are vetted and issued with security clearances. However, the Auditor-General consistently raises the concern that the intelligence

services' secrecy requirements does have some impact on their work. For example, when checking expenditure on intelligence operations, they cannot verify independently the existence of sources the services claim to have paid, or secretly acquired assets, as these must be shielded from public knowledge to protect operations. In response, the services argue that such is the nature of intelligence work, and that there will always be limits to what can be disclosed to the Auditor-General. For example, informants would be reluctant to provide information to the services, if their role and identities had to be revealed to the Auditor-General.

THE NATIONAL ARCHIVES

Another vehicle for the public to access information is through the records of the National Archives. This avenue should be of particular interest to historians, as well as members of the public wanting to access personal files. The National Archives Act of 1996 makes provision for the release of records after 20 years. As the national archivist has streamlined procedures in order to be aligned to PAIA, members of the public can use PAIA to access records in the custody of the National Archives.

The national archivist has already published a list of the files in its possession, and the names of people on whom the apartheid security services kept files. Affected persons were invited to view their files using the mechanisms under PAIA, if these files were older than 20 years old. The national archivist has a duty to ensure that the exemptions of the PAIA – particularly those relating to third-party information – are taken into account before releasing information. In terms of the National Archives Act's 20-year rule, intelligence service records created in 1995 would have to be transferred to the National Archives at the end of 2014. This implies that all records deemed public records in terms of PAIA would fall under the custodianship of the National Archives, including personal files, intelligence assessments, and administrative documents that have not been identified for disposal. Theoretically, it should no longer be possible for an intelligence agency to destroy sensitive records, as NIS did at the end of the apartheid era. However, while the services reportedly believe that they comply with the record management standards of the National Archives, there is no independent oversight to assess whether records are adequately filed, stored and preserved, for the sake of posterity and of conserving South Africa's collective memory.

DEPARTMENTAL REVIEWS

Since 1995 the executive, through various intelligence ministers, has initiated a number of reviews, some internal and some intended for eventual public disclosure. In most cases, the initiating authority has tried to ensure objective and independent proceedings by appointing prominent and credible outside observers to head or serve on the review teams. For the executive, these reviews have been an important vehicle for addressing emerging policy concerns in the intelligence services. The first known review was the Pikoli Commission, named after its chairperson, Advocate Vusi Pikoli. Initiated by Joe Nhlanhla, deputy minister for intelligence, in 1996, barely a year after the new services were established, the Pikoli Commission was in reality an internal departmental review. Establishing the services had been a rocky road for the deputy minister. It was difficult enough to amalgamate and streamline a bureaucracy that contained former foes, suspicious of each other despite having worked so hard to overcome their differences in the interest of national unification. But dealing simultaneously with the security problems of a fragile democracy (a resurgence of domestic violence in KwaZulu/Natal and on the Witwatersrand, an increase in organised crime, a perception that foreign intelligence agencies were spying on South Africa) and other internal vulnerabilities such as the theft of a convoy of vehicles and of a batch of computers containing sensitive information, was too much. These last two incidents were a huge embarrassment to Nhlanhla, and President Nelson Mandela threatened to shut down the intelligence services. Nhlanhla therefore decided that it was time to take stock.

The review focused on whether the mandate and design of the services as constituted were appropriate for the times. It also addressed how organisational effectiveness could be improved. The recommendations confirmed that the organisational design was appropriate but emphasised that new capacities, including signals intelligence, needed to be built. The need for improved training and human resource management systems was also identified. Although releasing the commission's recommendations would not have jeopardised national security, Nhlanhla chose not to table the findings or recommendations for discussion in parliament, raising the ire of opposition political parties. Instead, the recommendations were sent to the JSCI, who disclosed them in their report to Parliament the following year. Perhaps Nhlanhla was simply following due process; however, the perception created was that the intelligence services were on the defensive and unwilling to allow public debate about their organisation. Nhlanhla accepted the commission's recommendations and used them as a basis for his programme of work over subsequent years.

The dust had barely settled around the Pikoli Commission when the services were embroiled in yet more drama. This time General George Meiring, head of the SANDF, received information from Defence Intelligence that several prominent ANC leaders and a senior SANDF officer, General Siphiwe Nyanda, were plotting a military coup against President Mandela. Meiring took this report directly to Mandela, by-passing NICOC. It is conceivable that Meiring thought he was doing the right thing by circumnavigating his NICOC colleagues who might have been party to the alleged mischief. But the president dismissed the claims as ludicrous, and queried why it had been presented to him in such an irregular fashion. Again, Nhlanhla was forced to appoint a commission. After sitting for several months, the commission presented its results, which recognised that the co-ordinating legislation had to have been flawed to have been subverted in such a way by Meiring.

Further reviews were initiated under Lindiwe Sisulu, minister of intelligence from 2001 onwards. One of these had an internal focus and looked at the conditions of service of members of the intelligence community. It addressed the broader policy question of the status of the intelligence services in relation to the wider public service. After extensive interaction with the public service, the cabinet approved in principle the establishment of an Intelligence Services Council to look into this issue, asserting that the conditions of service for members of the intelligence community fell outside the public service's jurisdiction.

Other policy-related questions investigated by commissions initiated by Sisulu included the need for a classification and declassification framework aligned to the constitution, and the regulation of the private security industry. Other matters related to the sensitive work of the intelligence services, including the former government's chemical and biological warfare programme. In all cases the commissions made recommendations that were meant to inform policy decision-making or formulation.

One flaw in the system of government has been the lack of continuity, with a succession of ministers bringing their own ideas about particular policy priorities and directions. It reveals the disadvantage of having limited public participation or interest in the reviews, as ministers generally are not under public pressure to bring policy processes to a head. When appointed minister for the intelligence services, Ronnie Kasrils promised to pursue the policy concerns of his predecessor, including a classification and declassification policy. However, the political and security demands during Kasrils's tenure meant that other priorities took precedence, with the result that the classification and declassification policy remained on the agenda but was not treated with urgency. His term of office ended before the legislation relating to declassification and classification had been passed.

The most significant review under Kasrils was the Ministerial Review Commission on Intelligence. Appointed in 2005, it was tasked with assessing whether the operations of the intelligence services were aligned to the constitution. The three-person commission was headed by a former deputy minister for safety and security, Joe Mathews. In its final report, submitted in 2008, it strongly recommended tighter executive control over and scrutiny of operations initiated by the intelligence services.

The review followed the dismissal of several senior NIA managers, including the director-general, for allegedly conducting unlawful surveillance and providing false information to the president of the republic. The Inspector-General investigated and confirmed these allegations, which resulted in criminal charges being brought against the director-general, Billy Masetlha and others. However, a bitter and protracted series of legal battles ensued, as the former director-general fought to clear his name. Consequently, the courts emerged as a critical space in which matters affecting the intelligence services unfolded. Given the political climate, the media has become a secondary channel through which the developments in the intelligence services are filtered and aired.

In the earlier days of the new intelligence dispensation, problems within the intelligence services were rarely addressed by resorting to the courts, and almost never involved such senior personnel. There was the occasional case where a member of the intelligence services was charged with criminal conduct, and his links to the services exposed, but these incidents were generally benign and rarely covered by the media. There had also been incidents where aggrieved members or former members had turned to the courts for assistance over labour disputes that they had failed to resolve with management. The resort to the courts was hardly surprising in many cases, as the services had no access to the conciliation and mediation mechanisms available, having been expressly excluded from the provisions of the Labour Relations Act. In several cases, the incidents reached the courts because the employer-employee relations were poorly handled. Although some such matters were heard *in camera*, in most cases the disputes attracted little media interest and were settled out of the public glare.

MEDIA AND COMMUNICATION STRATEGIES OF THE INTELLIGENCE SERVICES

The intelligence services have always been sensitive to public perception. In 1995 the NIA appointed a senior manager as head of communications. This continued a trend that had become well established under NIS, which had allowed its

most senior officials to engage with the media in order to explain and demystify themselves.

However, media coverage has not always been kind to the intelligence services. Intelligence activity inevitably seems to generate a climate of suspicion. In 1996, allegations were made in the media that the intelligence services were spying on the top management of the SAPS. Over the years, other allegations were made in the media that the intelligence services were bugging the telephones of citizens, including opposition politicians. The stories of mishaps, ineptitude, and scandal carried in the media have made for titillating reading. The bungled spying on the German Embassy in Pretoria, and the theft of minibuses and computers from the NIA's headquarters, all made for good media copy in the first few years of the services' existence.

In response, the intelligence services have established capacities to manage their public image and public relations. Initially, the minister did not play a direct role in media interactions; the senior manager appointed by the service handled questions and queries from the press. Later, in order to standardise and exercise control over responses to media queries, Deputy Minister Nhlanhla appointed a spokesperson in the ministry to handle all media queries. This arrangement became embedded quickly enough and the office of the Minister now manages public relations for the intelligence services.

Nevertheless, the intelligence services do enjoy some autonomy in respect of communication strategies. Both the NIA and SASS have informative websites. Between 2001 and 2004 the NIA produced three comprehensive public annual reports that are available on its website at www.nia.gov.za. Vusi Mavimbela, a new director-general appointed in 2001, was particularly enthusiastic about improving the public profile of the Agency. Mavimbela says in his foreword to the 2002/3 public annual report:

> When we launched our Public Annual Report last year, we were driven by the simple conviction that the South African society is the ultimate stakeholder on issues of national security. It was the conviction that if this stakeholder is to play its role in ensuring national security for itself, it has to be informed of what the place and role of the National Intelligence Agency (NIA) is in society.

Through the reports, the NIA released significant and sometimes detailed information about itself and its work. For example on the subject of vetting, the 2001/2 report stated that the NIA had received in the past year 3 180 requests for security clearances, conducted over 16 000 record checks for special events, and issued a total of 1 379 confidential to top-secret clearances. The report listed the special

events provided with security advisory services, including the World Conference against Racism and the Inter-Congolese Dialogue. It stated that similar services would be provided over the coming years to the conference of the Non-Aligned Movement Summit, the World Symposium on Sustainable Development, the Summit of the African Union and the World Cricket Cup, all events taking place on South African soil.

The NIA's public annual reports also explained changes in priorities over the years. For example, in its 2003/4 report, border intelligence, organised crime and corruption and terrorism are reflected as priorities. The reports listed the types of 'products' (assessments) produced by the NIA, which included at the time daily and weekly intelligence reviews. Finally, the public reports provided statistical information about the demographics and composition of the NIA and its corporate governance framework. The timing of the NIA's last public annual report coincided with the resignation of Mavimbela and his replacement by Billy Masetlha. The disruption caused by the change in minister and director-general after the 2004 general elections may be the reason why no more public reports were produced. However, the fact that the NIA is not legally obliged to publish a public annual report means that there was never any leverage to ensure that this practice continued or was resumed.

In contrast, the SASS has produced only one public report – a glossy ten-year review. This fairly revealing document can be found on the SASS website at www.sass.gov.za. Like the NIA's reports, it covers the legal framework and mandate, provides demographic details (ratios not numbers) and explains the priorities of the Service. The report also explains the SASS's intelligence-gathering role in support of African peace initiatives, its co-operation with the law enforcement agencies in respect of crime intelligence, its work in economic intelligence, and its international co-operation with other intelligence agencies. However, since its voluntary decision to publish a ten-year review, the SASS has not continued to publicise its record in this way, and there is no pressure for it to do so.

The ministry itself is subject to the overall government communications strategy, led by the Government Communication and Information System (GCIS), which is located in the Presidency. The GCIS co-ordinates government communications including the schedule of press briefings, which cabinet ministers and their 'cluster' colleagues must attend. For communication purposes, the intelligence services fall under the Justice, Crime Prevention, and Security Cluster. Thus the minister regularly briefs the media about events in relation to these portfolios together with his or her colleagues. Over and above this, the minister engages with

the media on a range of security questions, granting interviews, meeting editors, and writing articles and letters.

CONCLUSION

Since 1995, the veil appears to have been lifted significantly on the intelligence services, with the public able to access information through a multiplicity of means. However, anecdotal evidence suggests that few citizens have the kind of insight required for regular monitoring and use of all these means. Public interest is not excessive, and is mainly stimulated by media reports, especially of a sensational nature. Policy priorities change from minister to minister. More processes are introduced to address the new priorities before the old ones have been completed, adding to confusion about the status of policy, even among the enlightened.

On reflection, the intelligence services have been generally transparent but have also been inconsistent. Examples include the discontinuation of public annual reports by the services and the relatively low profile of the work of the JSCI. What is perhaps needed is a transparency review, led by the minister, to take stock of what has been achieved and to look at how to maintain a consistent culture of transparency.

5

PAIA AND ITS IMPLICATIONS FOR THE INTELLIGENCE SERVICES

The Bill of Rights in the South African constitution states that every person has the right of access to any information held by the state, as well as any information held by another person required for the exercise or protection of any rights (s32.1). It states that national legislation must be enacted to give effect to this right (s32.2).

It also states that the rights in the Bill of Rights may only be limited if the limitation is 'reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom', and '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' (s36.1).

This is an important provision. In lay terms it means that the rights in the Bill of Rights are not absolute but can be restricted if the reasons for doing so can be argued with some legitimacy. In fact, as we will see, this is provided for in PAIA, which contains a set of grounds on which access to records can be withheld from requesters.

In 1994 a task team was established in the office of the then deputy president, Thabo Mbeki, to draft the legislation. Convened by Advocate Mojanku Gumbi, it also comprised Advocate Vincent Maleka, Professor Mandla Mchunu, Professor

Etienne Mureinik, and Advocate Empie van Schoor, a state law advisor. Its brief was to draft a law that would cover access to information, access to meetings, and the protection of whistleblowers.

Recounting the drafting process, Van Schoor confirms that the principle of maximum disclosure was paramount during early deliberations (interview, 25.08.03). The task team studied access to information legislation of several countries, including Australia, New Zealand, Ireland, the United States, Britain (in draft form at that time), and India (also in draft form). They met regularly to discuss various drafts.

In a document dated 19 January 1995, the task team noted that 'certain classes of sensitive information' would have to be exempted from disclosure. These should be narrow, well-justified, designed to prevent real harm, and, where necessary, subject to a public interest override. In its initial draft the task team proposed exemptions in cases where the release of information could cause serious harm to national defence or security; undermine law enforcement; jeopardise personal privacy, the safety of an individual; endanger the government's management of the national economy or the national finances, or affect the government's capacity to collect information in the national interest, proper personnel administration in the public service, or the deliberative process within the government by inhibiting candid internal communication (Open Democracy Task Team 1995).

The initial proposal also required public bodies to take proactive steps to foster a culture of transparency. The task team argued that such bodies should routinely publish or make available the following kinds of information: manuals or brochures detailing descriptions of the classes of information in their possession; their internal structures, functions, responsibilities and decision-making processes; the means by which citizens could participate in the decision-making processes; details of available complaint, appeal and redress procedures; details of available public services and how to use them; and details of internal complaints procedures available to an official wishing to draw attention to lawbreaking, corruption, or maladministration.

Among the enforcement mechanisms proposed by the task team was the appointment by each government body of an information officer who would consider requests for information. Should a request be refused, the requester could appeal internally to the head of the public body. In the event of an unsuccessful internal appeal, a requester would have recourse to an information court that dealt exclusively with the enforcement of the Open Democracy Act. The public protector and human rights commission would be granted intervention and mediation powers. The task team also proposed that an independent body (the Open

Democracy Commission) be established to monitor the effectiveness of the Act and to report annually to parliament on its implementation through the appropriate parliamentary committee.

The drafting of the Open Democracy Bill proceeded with periodic delays. Between 1995 and 1996 it was submitted twice to the cabinet, but was referred back each time for further work and consultation. In October 1997 the draft bill was published in the *Government Gazette* for public comment. Comments were considered, further adjustments were made, and in 1998 cabinet approved the draft. In 1998 the bill was finally tabled in parliament. The purpose of the Open Democracy Bill was to give citizens access to information held by public bodies, and access to the proceedings of certain public bodies. Other aims were to protect privacy, and to protect officials who disclosed serious maladministration or corruption. Overall, the bill would empower the citizenry to participate in governmental decision-making that affected them (Currie & Klaaren 2002).

The original recommendation was for a single act to accomplish the work 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, the cabinet decided to table a separate bill that dealt with whistleblowers and open meetings, and over time abandoned the open meetings component. The legislation dealing with whistleblowers was the Protected Disclosures Act of 2000. Van Schoor explains that the reason for having a separate bill was constitutional, as technically the constitution required the access to information legislation to be enacted before 4 February 2000 (interview, 25.08.03).

The Promotion of Access for Information Act (PAIA) was finally passed by parliament in 2000. This law gives substance to the constitutional right of access to information held by the state. Its stated aim is the following:

> 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 (PAIA, Aim).

AN OUTLINE OF PAIA

PAIA requires that all public and private bodies release information about themselves, list information or records they hold, and state how members of the public can access those records. It also outlines the grounds on which public and private bodies may refuse access to their records, and provides mechanisms for appealing against such decisions.

The scope of the Act

The Act overrides any legislation that might be materially inconsistent or in conflict with its provisions. This implies that the intelligence services cannot claim an automatic right to secrecy, and must balance their objectives (also defined in law) with the provisions of the Act. However, there are grounds for legitimate and justifiable non-disclosure, which are covered later in this chapter.

The Act states that information held by the state should be made public 'as swiftly, inexpensively, and effortlessly as reasonably possible without jeopardising good governance, privacy and commercial confidentiality' (s9b).

However, not all public bodies are subject to PAIA. Section 12 stipulates that the Act does not apply to records 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 of 1996; and officers of such courts or tribunals. Nor does the Act apply to individual members of parliament or provincial legislators. However, it does allow the cabinet and its committees, members of parliament, or provincial legislators to request information about private bodies.

The Act provides mainly for access on request and, in particular, for access to already existing records. Therefore, the body that receives a request cannot legitimately be expected to compile a record, if a record does not exist.

The Act is strongly weighted in favour of those requesting information. The constitution does not require a requester to prove that the information is necessary for the exercise of their constitutional rights. In fact, the reason for the request is irrelevant; the onus is on the public or private body to whom a request is directed to comply with any legitimate request, if there is no legally based reason for withholding a requested record.

Routine disclosures required in the PAIA manuals

The Act (part 2, chapter 3, s14) outlines the information that all public bodies must publish in a manual in at least two official languages. (Part 3 lists identical requirements for private bodies.) The manual must contain a description of

the public body's structures, functions, and contact details; a list of the records held, by subject and categories of each subject; and a description of every personal information bank held by the public body. It must also clearly state which categories of records are open to the public, and how to obtain access to those records; describe its services available to members of the public; and how to gain access to these services. It must also describe arrangements for members of the public to participate in or influence the formulation of policy, or the exercise or performance of duties (Currie & Klaaren 2002).

Section 14, through the requirement to produce manuals, is the window through which members of the public can gain much insight into the role, structure, and functions of the public body in question. It is probably more significant in respect of the intelligence services than other public bodies, into which members of the public are likely to have some insight through media reports and generally available information. The secrecy surrounding the intelligence services tends to be perpetuated by the routine classification of most information and the absence of a framework for the non-classification or declassification of such information, a condition which could be significantly alleviated by the availability of manuals.

Requests for access to information

PAIA requires that all relevant public bodies appoint a deputy information officer (DIO) to attend to its obligations under the Act. Thus the DIO is directly responsible for processing requests for information, as well as transferring requests if the public body does not have the required information. Agencies are required to ensure that requests are kept until a final decision has been taken on whether or not to grant access. No official of a public body, other than the information officer or deputy information officer, has the power to respond to a request for access.

Grounds for refusal of access to records

PAIA recognises that there are circumstances under which public bodies should have the right to refuse requests for information. In the first instance, refusal is deemed to have taken place when the body in question replies that a requested record cannot be found or does not exist, or when the response to a request is not lodged within the regulated time. Should a request be refused, an appeal can thereafter be made, first to the body and then to the minister. Another significant feature of the Act is that an information officer may deny the existence or non-existence of a record, if the public body believes that acknowledgment thereof is going to cause harm (part 2, chapter 4).

The grounds for legitimately refusing access to a record are clearly stipulated, and must be justifiable in terms of the constitution. Both mandatory and discretionary grounds for refusal are provided. In the case of the former, a body must refuse access to requested records. In summary, a request for access to a record may be refused if the refusal is based on the mandatory protection of privacy of a third party who is a natural person; tax and certain other records held by the South African Revenue Services (SARS); commercial information about a third party; the safety of individuals and of property; police dockets; or research information.

There are also a number of discretionary grounds for refusing access. In other words, the public body receiving the request must evaluate whether the request will compromise certain of its responsibilities. A request for access to a record may be refused if the refusal is based on the protection of certain confidential information about a third party; law enforcement and legal proceedings; or defence, security, and international relations of the Republic. Access may also be refused if 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 the information is in the public interest, or would reveal substantial environmental risk or harm to public safety (Currie & Klaaren 2002).

Implications for the intelligence services of the grounds for refusal

Given that the intelligence services are subject to PAIA, the implications of each of these grounds for refusal need to examined. The overall result is a legal environment in which there is considerable room for the intelligence services to protect their secrets.

Mandatory protection of the privacy of a third party who is a natural person

This provision, in section 34 of the Act, is meant to protect an individual's privacy, a right also enshrined in the constitution. The clause implies that a public body cannot provide a requester with personal information about a third party, which includes a deceased person. Nonetheless, access may be granted in certain cases – for example, if the person concerned has consented to disclosure, or 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 relates to the physical or mental health of a third party minor under the care of the requester. Finally, access may be granted if the information is about an

individual who is or was an official of a public body, and relates to their position in relation to the office.

This clause implies that the intelligence services are not allowed to make available to requesters personal information about persons in their ranks, who work as agents or informers, or who are the targets of intelligence collection without the consent of the individual concerned. This supports the requirement that the identities of intelligence workers and their sources must be protected, which is already provided for in the Intelligence Services Act of 2002.

However, persons on whom apartheid-era security services had kept files could request to see their own files in terms of PAIA if the records were more than 20 years old, as prescribed in the National Archives Act of 1996. In November 2003 the National Archives took the unprecedented step of publishing a list of files which had been maintained by the apartheid security forces, and invited the people listed to apply for access to their files in terms of PAIA. However, no member of the public was entitled to see another person's file unless the person concerned had agreed in principle to such access. After evaluating the request, the files could then be released to the requester provided they did not contain information that was protected in terms of PAIA. The National Archives stressed that any person seeking access to their personal file kept by the security forces would have to comply with PAIA's requirements, complete the necessary forms, and pay the prescribed administrative fees for processing the request.

This ground for refusal is also relevant to the security screening of public servants. Intelligence services routinely use detailed screening processes to acquire information about new employees, as well as unsuccessful candidates. They are also sometimes asked to investigate and issue security clearances to civil servants who have routine or frequent access to sensitive information. In general, reasons are not supplied when candidates fail to obtain security clearances. Though PAIA has not been tested in respect of security clearances, this may have to change, or at the very least the intelligence services would have to document carefully such reasons, in case an individual requesting access to the records challenged the decision.

This provision of PAIA implies that the intelligence services should protect the privacy of such candidates. The broad guideline is that it would be illegal to provide personal information to a third party without the consent of the individual concerned. While South Africa does not have privacy legislation, this protection of personal information is in line with the South African Law Commission's draft concepts on privacy legislation.

Mandatory protection from disclosure of certain records of the South African Revenue Service

According to section 35 of the Act, SARS must refuse a request for access if the record contains information obtained or held for the purpose of enforcing tax collection legislation. Although this reason for refusal may at first glance not appear to have direct consequences for the intelligence services, it does, especially when one considers that a substantial part of any intelligence services' budget is for the remuneration of informers, often the life blood of their operations. SARS's effectiveness depends on being able to match an individual's bona fide identity with his or her income. As intelligence agencies often make use of persons or entities with false identities for the purposes of operational security, this poses a dilemma. Should such remuneration for services be regarded as 'income', and if not, why not? At the time of writing this issue had not yet surfaced publicly, and is therefore raised hypothetically. But it may well do so in future, when a sound and legally defensible regime around the remuneration or income of sources will have to be developed. From a public interest perspective, whether such disbursements are taxable or not, what is at issue is whether such payments to sources are reasonable, duly authorised, and the procedures effecting them transparent enough to prevent corruption.

Mandatory protection of commercial information of a third party

According to section 36 of the Act, a public body must refuse a request for access if the requested record contains trade secrets involving a third party; financial, commercial, scientific or technical information which, if disclosed, could harm the commercial or financial interests of a third party; or information supplied in confidence by a third party which, if disclosed to a requester, might harm its 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, if the third party in question has consented to the information being made available, or, if disclosing information relating to product or environmental testing would reveal a serious public safety or environmental risk. This clause is relevant to the intelligence services in that they routinely enter into contractual arrangements with commercial entities. In some cases, especially where some operational matter is at risk, commercial entities have to keep their relationship with the intelligence services secret, and are often required to undergo security clearances and due diligence procedures before being confirmed.

Mandatory protection of certain confidential information, and protection of other confidential information about a third party

Section 37 stipulates that a public body must refuse a request for access to a record if disclosing the record in question would constitute a breach of confidence in respect of a third party in terms of an agreement. It may also refuse access to records that contain information supplied in confidence, whose disclosure could 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 relevant to the intelligence services as much of their information is procured from confidential sources or informants. In most cases, sources undertake to supply sensitive information on condition that their identities will not be disclosed. Although not tested, this clause may in fact be relevant when considering whether information relating to payments of sources may be withheld from SARS, a point discussed earlier.

Mandatory protection of the safety of individuals, and protection of properties

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

This exclusion correlates strongly with the provisions of the Protection of Information Act, which seeks to prevent and penalise the disclosure of information with similar effects. Thus the intelligence services, which do provide security advice to government departments and therefore must be presumed to have such information at their disposal, would be within their rights if they refused to disclose information that prejudiced the safety of an individual or the public or the security of a building, structure, communications system, transport system, or property.

Mandatory protection of police dockets in bail proceedings, and a protection 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. Refusal is also allowed under certain other conditions, for example, if the record contains information about investigative methods and techniques, and its disclosure may prejudice the effectiveness of the investigation, or may reveal or provide leads to the identity of a confidential source of information.

This clause is relevant to the criminal justice and intelligence sectors. Information can be withheld in the interests of a successful outcome to an investigative process. However, the Act is sensitive to other basic freedoms: in the same clause, it states that a requested record may not be refused if it contains information about the general detention conditions 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 carefully stipulates the elements of a satisfactory response, and the requester also has the option of lodging an internal appeal.

Mandatory protection of records privileged from production in legal proceedings

Section 41 states that a 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. Legal professional privilege is a general legal principle that protects the integrity of legal proceedings by protecting the confidentiality of communications between a lawyer and his or her client. In theory, records that might be the subject of a request include correspondence or communications made for the purposes of giving or seeking legal opinion and advice. The intelligence services can invoke this ground for refusal should its records require protection.

Discretionary protection of information related to the defence, security and international relations of the Republic

According to section 41, a public body may refuse access to a record if its disclosure could prejudice the defence, security, or international relations of the Republic; 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.

This would include information about military tactics or strategy, and military exercises or operations to prepare, detect and prevent hostilities; information relating to weapons procurement, capacity and development; information concerning force deployment and characteristics; and information held for intelligence purposes.

In this respect the Act again seems aligned with the Protection of Information Act. In fact, these and other provisions are quite generous in ensuring that the intelligence and security services are not disabled. They are sufficiently broad to refuse disclosure, and allow the public body's information officer some discretion over whether to disclose information or not. The information officer may also

refuse to confirm or deny the existence or non-existence of a record, if it is thought that either refusal or denial would harm the interests of the state.

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 Act, access may be refused when 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 in the best interests of the Republic. This could include information about proposed policy changes affecting currency, coinage, legal tender, exchange rates or foreign investment; the government's position in respect of 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.

Mandatory protection of research information of a third party, and protection of research information of a public body

In terms of section 43, when a third party could be exposed to serious disadvantage, a record that contains information about research being conducted by or on behalf of the third party may be withheld. This provision could presumably also be used by the intelligence services, whose intelligence reports are client-driven. They could argue that a client, such as the president of the Republic or the cabinet, could be disadvantaged if the studies commissioned are made public.

Discretionary protection of the operations of public bodies

In terms of section 44, information can be withheld from public disclosure if the record 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.

In essence, this provision serves to shield the public bodies from scrutiny of their inner workings. Intelligence agencies could readily use it to ensure that sensitive minutes or policy documents are not made publicly available.

Discretionary protection from manifestly vexatious or frivolous requests

Section 45 states that a request for access may be refused if a request is manifestly vexatious or frivolous, and the work involved in processing the request would

divert substantial resources. Any public body refusing access to a record on these grounds would have to consider carefully what constitutes a frivolous request, to countermand the requester's argument that the information is important to it. In any event, PAIA does not require a requester to justify reasons for wanting access to a record. It is simply an incontestable right if the information or record requested is not covered by the grounds for refusal.

Mandatory requirement of disclosure if it is in the public interest

Lastly, section 46 of the Act provides for mandatory disclosure if the record were to reveal evidence of serious contravention 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. A requester may launch an internal appeal with a public or private body that refuses access to information, within stipulated time frames. If unsuccessful after exhausting the internal appeal procedure, 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 if appropriate. The burden is on the refusing body to demonstrate the veracity of its decision. These conditions – confidential presentation of argument – work in favour of the intelligence services.

Functions of the Human Rights Commission (HRC)

Part 5 of the Act addresses the functions of the HRC in relation to the Act. The HRC is charged with making the Act known to the public and monitoring its implementation. It also has to train the information officers of public bodies, and provide advice on how to administer the Act. The HRC must make recommendations for developing, improving, modernising, reforming or amending the Act, or other legislation or common law relevant to access to information held by private or public bodies. And, every year, the HRC has to provide detailed reports to the National Assembly on how well each public body is implementing the Act.

Other aspects covered by the Act

Part 6 covers transitional provisions, which include the minister having to introduce legislation to ensure that Schedules 1 and 2 of the Act are completed. It also provides for extended periods to deal with requests during the first two years.

Part 7, the last part of the Act, covers general provisions. It stipulates that any person who attempts to deny a right of access by wilfully destroying, damaging, altering, concealing or falsifying a record is liable for up to two years' imprisonment. It also stipulates that the minister must provide regulations for the Act's implementation, and submit them to parliament before publication. Provisions of the Act may be brought into operation on different dates.

Cabinet records

This analysis of the grounds for refusal shows that PAIA, notwithstanding its intention of facilitating access to information, provides ample space for information to be withheld from requesters. This seems to support concerns that the Act could in fact be used to frustrate attempts to access information. Moreover, cabinet records are excluded from access. The implications of this are debatable. On the one hand, the executive in a democracy must be assumed to have legitimacy and a mandate to govern. On the other hand, where it takes decisions with far-reaching implications for the state as a whole, there is likely to be a backlash against unpopular policy moves. It was under the cover of cabinet prerogative that many harmful decisions were taken under apartheid: this much emerged during the hearings of the TRC. It is therefore in the broader public interest for access to executive decision-making to be as meaningful as possible.

PAIA'S IMPACT ON THE INTELLIGENCE SERVICES

This section deals with the attempts of the intelligence services to balance the competing requirements of secrecy and transparency, while taking PAIA into account. It also assesses whether these actions have contributed to effective and accountable governance of the services, and analyses the policy choices resulting from the Act, as expressed in institutional arrangements and statements by policy-makers.

President Thabo Mbeki assented to the PAIA on 2 February 2000. Originally scheduled to come into effect on 15 September 2000, the Act was delayed until March 2001 to enable the drafting and approval of regulations. The first draft interim regulations were published on 10 August 2001, and certain sections of the Act came into force on 15 February 2002.

Implementation

However, implementation proceeded slowly. For example, public and private bodies were generally slow in responding to the requirement to submit manuals.

(As noted earlier, the Act requires public bodies to produce manuals containing detailed information about their structure and functions, the information they hold, and how these may be accessed by members of the public.)

When the government noted that both public and private bodies were not adhering to the requirement to produce manuals, the due date for giving effect to this provision was extended to 28 February 2003, by way of a blanket exemption for all public and private bodies. Even by this date, very few government departments had met the deadline. In 2003 the minister of justice and constitutional development granted a further reprieve, exempting public bodies and private bodies from submitting manuals for the period 1 March 2003 to 31 August 2003. The ministry for intelligence services co-ordinated applications by the SASS and NIA for an exemption from the manuals requirement. Both departments stated that complying with this requirement would compromise their mandates, and jeopardise national security. The minister for justice and constitutional development granted the exemptions. Both SASS and the NIA were exempted from compiling manuals for the period 2003 to 2008 (interview with Marlyn Rasswisi, 4.08.05).

Advocate Empie Van Schoor, former member of the open democracy task team that drafted the access to information legislation, is critical of the fact that the regulations were not finalised until several years after the Act had been passed, and argues that one of the lessons of the process was that legislation and regulation should be drafted simultaneously (interview, 25.08.03).

However, David Porogo, DIO in the Department of Justice and Constitutional Development (DOJ), blames the delay in implementation on other factors. According to him, implementation was not linked to the department's budgeting process, despite the department having overall responsibility for implementation, which affected practical measures, such as developing and distributing educational material. Furthermore, many heads of department were unaware of the Act's provisions, such as their own roles as information officers, the requirement to appoint DIOs, or the requirement to produce manuals. In that sense, the intelligence services were no more guilty of non-compliance with the Act than many other departments (interview, 27.08.03).

By August 2005, the NIA and SASS displayed different degrees of readiness for implementing the PAIA. By that stage the NIA had produced a document entitled 'Policy on the Procedures on the Disclosure of Information' that regulated its implementation of the Act. NIA did in fact appoint a DIO, responsible for ensuring proper administrative compliance with the Act, compiling responses (to requests) for consideration and approval by the Information Officer (IO), and any other duties relating to PAIA compliance delegated by the director-general.

However, the policy as a whole was classified 'confidential' and was therefore not publicly available to those seeking to understand the NIA's request procedure.

SASS, on the other hand, only had a draft policy, which was also classified 'confidential'. At the time its director-general still had to approve the policy, and had not appointed a DIO. According to the director-general, Hilton Dennis, the draft policy on information management was more concerned with identifying which information required protection than with the procedures covering requests for information (interview, 25.07.05). As such, it was intended to be aligned, but not concerned exclusively, with the implementation of PAIA.

By contrast, the Department of Defence (DOD) had a policy that outlined roles, responsibilities, and mechanisms for implementing PAIA. It had been approved by the highest policy-making body in the DOD, the plenary defence council. The DOD's structure had two components: the secretariat, falling under the secretary for defence, who is also the accounting officer for the department; and the SANDF, headed by its chief. The secretariat and defence force each have their own management and accountability structures, both leading up to the minister of defence. On a monthly basis, the plenary defence council brings together the most senior management of the two components and is chaired in alternate months by the secretary for defence and the chief of the SANDF (interview with Wayne Hendricks, 28 July 2005).

According to Hendricks, a former DOD official, the policy regulating PAIA implementation in the DOD was approved in 2000 (interview, 28.07.05). The policy was classified as 'restricted', and its handling instructions stated 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, promulgated by the DOD in 1999, in response to the tabling in parliament of the Open Democracy Bill. As accounting officer, the secretary for defence was designated as an IO, while DIOs were to be the heads of the SANDF and the secretariat. In line with the PAIA provisions, the policy described the IO's role: to appoint, direct and control the DIOs; to render, or make available, such reasonable assistance required by 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.

The policy also described the DIOs' responsibilities, which included the following: to develop internal procedures to implement the Act in their areas of responsibility; to ensure that persons with delegated responsibilities were trained in the Act's procedures and stipulations; 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 (IAAC) 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.

The IAAC consisted of representatives of the IO (who would chair the committee), the SANDF chief, the legal support directorate, defence intelligence, and the head of the information centre. Its role was to advise the IO on recommendations from the DIOs regarding requests for information.

According to Hendricks, the Justice College, under the Justice Department, had trained DOD representatives from different divisions. Available to all government departments, the week-long training emphasised the constitutional basis of PAIA, and the presumption in favour of disclosing all public records, except in those cases where exemptions were provided for in the Act (interview, 28.07.2005).

The challenge for the NIA, SASS, and the DOD was to provide adequate resources to implement PAIA. In NIA, although the DIOs were members of senior management with other vital responsibilities, they did not have sufficient dedicated staff to follow up on PAIA requests. According to the NIA's primary DIO, Jackie McKay, developed countries such as the United States and Canada have well-resourced and staffed units responsible for ensuring effective implementation of access to information legislation. It was this lack of resources that resulted in the NIA sometimes failing to respond within the stipulated deadlines (interview, 15.07.05).

Compliance

The degree of compliance with PAIA by the intelligence services was examined during interviews with the director-general of the NIA, Billy Masetlha, (4 August 2005), and the director-general of SASS, Hilton Dennis (25 July 2005).

Both were aware of the main requirements of the PAIA but admitted that their departments did not comply with all of them, which supports the theory that the intelligence services are ambivalent about implementing the transparency required by the Act. However, they were open about their services' shortcomings, which perhaps reflects the growing awareness of the Act.

Appointment of deputy information officers

At the time of the interviews, the NIA had appointed and published the name and contact details of its primary DIO, in compliance with PAIA. However, SASS had not yet appointed a DIO. Dennis said it was considering appointing the general manager for information technology as DIO as he or she would be most aware of the nature of records held by the service, their classification, and their location in the department's various databases.

Voluntary disclosure

The NIA and the SASS comply to a certain degree with another requirement of PAIA, that of voluntary disclosure. Both have websites, although these are not updated very regularly. In June 2005 the ministry for intelligence services also launched a website, which it updated fairly regularly with the serving minister's speeches and responses to parliamentary questions.

The NIA and SASS have also released voluntary annual public reports. The NIA did so every year from 2001 to 2004 (after which the practice stopped), while the SASS published a ten-year review in 2004. Much of the information released relates to their mandates, functions, and corporate profiles. The NIA website contains the following categories of information: the NIA's 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; NIA's focus areas; the code of conduct for intelligence workers; and contact details. The SASS website had a similar structure, and includes the SASS ten-year review.

Every year these intelligence services also supply oversight bodies with information, evidence of which can be found in the annual reports of the JSCI and the Auditor-General. They have also initiated regular media briefings in an attempt to improve public understanding of their roles.

Reports to the HRC on requests received

Dennis admitted that his department had not complied with part 5 of the Act, which required that bodies subject to the Act submit reports to the HRC on the number of requests and appeals, and how they have been dealt with. However, Masetlha indicated that the NIA had met all such obligations. Dr Leon Wessels, an HRC commissioner, admitted that the HRC had not paid specific attention to the compliance of the intelligence services. The HRC faced a more general problem: that government departments at all tiers were unaware of the Act's provisions, and

did not have the resources to focus on the minutiae and special circumstances of the intelligence services (interview, 2.08.05).

Since the passage of the PAIA, the SASS had received no more than six requests, most of them from members of the former anti-apartheid activists requesting access to their files. In reply, SASS referred applicants to the NIA. Dennis explained that all surviving files from the apartheid era had been placed in the custody of the NIA in 1995, when the services were amalgamated. Therefore, if those records did exist, they would be in the NIA files.

By contrast, the NIA had received 43 requests for access to information since 1991: four in 2001, which were all 'positively responded to'; six in 2002, which were all 'responded to' (except for requests for TRC records that were referred to the DOJ); 12 in 2003, which were responded to either 'indicating that no information was available on the subject matter requested', or making the information available (there were no refusals); nine in 2004, of which the majority were submitted by the South African History Archives Trust on behalf of individuals, and there were no refusals. Until July 2005, the NIA had received 12 requests, the majority of which had been submitted by the South African History Archive (SAHA), mainly acting on behalf of prominent figures in the pre-1994 anti-apartheid struggle. Again, there were no refusals.

Most of the requests received by the NIA were for personal information, from anti-apartheid activists wanting access to their own files. SAHA intentionally played an important role, helping people lodge their requests with various government departments, so as to determine the state's capability, knowledge and attitude towards the PAIA. According to Masetlha, during 2002 and 2003 the 'initial requests' (with SAHA often acting on behalf of the requesters) were for sensitive records of the TRC; former BOSS files, which required submitting a very specific National Archives index to substantiate the request; and information on prominent anti-apartheid activists prior to 1990. The NIA also received requests, which were transferred to other public bodies holding the records, including the National Archives, the Office of the Auditor-General, and the Department of Justice and Constitutional Development.

6

THE INTELLIGENCE SERVICES AND THE RIGHT OF ACCESS TO INFORMATION: THREE CASE STUDIES

The three case studies presented in this chapter illustrate the dilemmas and choices facing the intelligence services when balancing secrecy (in the interests of national security) and transparency. One comprises a PAIA application by a non-government organisation, the South African History Archives (SAHA), for access to records that had earlier been presented to the TRC. The second comprises a PAIA request for records relating to the decisions of the Ministry of Defence in respect of a procurement tender. The third deals with politically explosive claims that a serving national director of Public Prosecutions had been an agent of the apartheid security apparatus. Both these issues served before institutions of the post-apartheid state. Each case presents the outline of events and choices made by the intelligence services in processing requests for records, and the responses of the requesters to their refusal of access. These case studies highlight the importance of valid, convincing grounds for any refusal, and emphasise the fundamental nature of the right of access to information.

APPLICATION BY SAHA FOR ACCESS TO TRC RECORDS

After the TRC process, SAHA, a non-government organisation committed to greater public access to records, lodged a formal request in terms of PAIA with the NIA and the Department of Justice and Constitutional Development (DOJ) for access to the records received and considered by the TRC. The request was declined in ways outlined below. As a result, on 26 November 2002 SAHA's lawyers served notice of its intention to apply for a High Court order setting aside

the decision of the minister of justice to refuse three internal appeals submitted earlier that year. Not only had the minister failed to respond to the internal appeals within the 30 days stipulated in the Act; but SAHA also believed the minister's refusal was procedurally flawed. Firstly, no reasons for dismissing the appeals were given to SAHA's deputy director, Sello Hatang, who had filed the application on SAHA's behalf. Secondly, SAHA argued that the delay in providing the applicant with decisions was neither fair nor reasonable. Thirdly, they argued that the way in which the applicant had effectively been denied access to the requested records was inconsistent with the constitution as well as PAIA.

The background is as follows: on 20 May 2002, SAHA's deputy director, Sello Hatang, submitted two requests for access to TRC records to the DOJ. The requests were made in terms of the provisions of PAIA. One request was for copies of all records held by the DOJ which documented the chain of custody of certain TRC records since their transfer from the TRC in 1999, including information about their location, physical transfer, control, responsibility, processing, and classification. The second was for copies of the transfer lists used to move TRC records from Cape Town to the National Archives in Pretoria. Hatang had previously sent a letter to David Porogo, DIO at the DOJ, informing him of SAHA's intention to launch a TRC archive project.

On 21 May 2002 SAHA sent a third and similar request to the NIA. The NIA replied in writing, stating that the TRC documents were not in their custody and were the DOJ's responsibility. It undertook to refer the request to the DOJ.

On 12 August 2002 Hatang received a letter from Porogo advising him that the requested documents could not be found. According to section 23(3) of the PAIA, a notice that records cannot be found or do not exist is regarded as a refusal of access. Consequently, SAHA lodged an appeal against the refusals with the minister of justice and constitutional development, on the grounds that Porogo did not seem to have applied his mind to the requests. SAHA also contended that Porogo had failed to adhere to the procedures in respect of the 'deemed refusals'. The Act stipulates that if the requested records cannot be found, the information officer has to provide an affidavit or affirmation that spells out in full the steps taken to find the records or to determine whether the records existed.

According to Hatang, the withholding was all the more intolerable because he was also in possession of a letter from the NIA which stated that it had no security or other concerns about granting the request for access to TRC chain-of-custody records, and providing such records to SAHA. A copy of the letter had been sent to the head of ministerial services in the DOJ on 24 October 2002.

The case of the TRC records was a protracted one. More than a year later, on 22 December 2003, Porogo lodged his replying affidavit to Hatang's application with the High Court, in which he claimed that he had been unaware of the whereabouts of the records in question when they were initially requested. He stated that:

> 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 (Porogo, TPD 22/12/2003).

According to Porogo, officials in the Ministry for Intelligence Services rebuffed his efforts to retrieve the documents, stating that the minister intended to review the documents as part of a classification and declassification process, which the ministry would initiate shortly. SAHA also rejected this argument, questioning why the ministry would be driving such a process when the DOJ was the responsible department.

Porogo's delayed response did not mean there was no activity around the contested records. In February 2003 the minister for intelligence services, Lindiwe Sisulu, established a Classification/Declassification Review Committee (CDRC) tasked with advising her on the best way to deal with the request. After considering the matter, the CDRC recommended that the review and release of all sensitive documents should be regarded as special projects, and approved by the minister. In this instance, the objective would be to review the sensitive documents (contained in 34 boxes) in accordance with PAIA's exemption clauses. Any document that did not require protection in terms of these clauses would be voluntarily released into the public domain. The CDRC also recommended the formation of an Interdepartmental Review Committee (IRC) to review the status of the requested records and consider their release. Marlyn Raswiswi, a member of the PAIA Unit in the DOJ, was appointed as the IRC's chair. The PAIA compliance process would be overseen by the CDRC (interview with Raswisi, 4.08.05).

In effect, the IRC would have to scrutinise each document and, based on standard criteria, recommend whether or not it could be released to SAHA. In his affidavit to the High Court, Porogo said this process only began on 9 September 2003 after certain preparatory measures had been completed. These included

gaining the approval of the special project by the ministers for Intelligence Services, Justice and Constitutional Development, and Arts and Culture (the last-named responsible for the National Archives); relocating the sensitive documents to the South African National Archives; establishing the IRC; training its members; and providing it with the necessary resources. The review process consisted of three phases: verification of the documents; their actual review; and oversight of the process.

The purpose of the verification process was to ensure that all the records which SAHA claimed existed could be accounted for. The process was guided by Dr Biki Minyuku, former chief executive officer of the TRC, assisted by personnel from the National Archives and former personnel from the TRC's records office. In 1999 Minyuku had been responsible for selecting and handing over to Dr Dullah Omar the 34 boxes of records which he believed to be sensitive.

Two inventories were used for the verification: one compiled by the TRC, which accompanied the sensitive documents in 1999, and a more detailed one compiled while 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, ie '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. (Replying affidavit to the High Court by David Porogo, 22 December 2003.)

Apart from the contested list of informers, some of the records fell in the category of Chemical and Biological Warfare. Many of these were already in the public domain as a result of the trial of Dr Wouter Basson, a surgeon in the SANDF, who had stood trial for his role in running secret projects using state funds, allegedly aimed at manufacturing chemical agents for use against anti-apartheid activists. Other categories of information related to files on the Steyn Commission; an investigation entitled 'Pro Jack'; the investigation into the murder of the 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 the former Swedish prime minister Olaf Palme, where most, if not all, the documents were in Swedish.

Porogo insisted that the IRC had reviewed the documents contained in the 34 boxes in accordance with the provisions of the PAIA. They were then reclassified into six categories, based on the sensitivity of the information and PAIA's

provisions. These included full disclosure (stamped 'declassified'), which meant all information contained in the document could be disclosed; partially disclosed (stamped 'declassified'), which meant that any information relating to PAIA exemption clauses was masked out, in accordance with section 28 of the Act, which dealt with severability; and no disclosure, which meant that the documents contained information which was exempted in terms of chapter four of the Act on grounds for refusal of access to records.

In some cases, records could be disclosed subject to third party notification. Information would remain closed until third party consent had been obtained. Finally, there was a category of records whose status still had to be determined. These documents would remain closed until clarity over their classification or verification had been obtained.

Porogo stated that the most common reasons for categorising documents as 'no disclosure' were to protect personal and third party information; methods, technical and manufacturing details pertaining to chemical biological warfare documents; and South Africa's relations with other states. Except for those documents requiring translation (which was in progress), the majority of records had been reviewed. His affidavit contained the following table, which showed the results of the categorisation process as at 5 December 2003:

SUMMARY OF CLASSIFICATION OF TRC RECORDS AS AT 5 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	30,40
TOTAL	1 684	100,00

In an interview, Raswiswi elaborated further on how the IRC worked. The IRC included representatives of the SANDF, NIA, the SAPS, and SASS, and had logistical support from the National Archives on whose premises the actual review took place. Most of the information withheld had been provided to the TRC on grounds of confidentiality. As chairperson, she tried to achieve consensus on the classification of each document. Once consensus had been achieved, she sought to ensure that the reviewed status was consistent with PAIA. The IRC completed its work

in January 2004, and handed its report to the CDRC (interview with Raswisi, 4.08.05).

Porogo's attorneys informed Hatang that copies of the documents could be inspected at the premises of the National Archives. They referred to a 411-page document entitled 'Worksheet for the review of the TRC documents', which summarised all the documents described as 'sensitive' contained in the 34 boxes. The worksheet was classified as 'confidential', as it described not only the declassified documents but also highly sensitive documents classified as 'no disclosure'. As the worksheet was developed during the review process for the IRC and CDRC, Porogo argued that SAHA was not entitled to a copy. However, he offered SAHA a copy of the worksheet under the condition of confidentiality, so that it could understand in greater depth the basis on which the DOJ decisions had been made.

SAHA rejected this offer on the grounds that it could not accept an 'in confidence' response to a request. In response, Porogo proposed that a member of his staff be present when the applicant and their attorneys inspected the documents at the National Archives, in order to explain why certain documents could not be disclosed.

In replying affidavits to the High Court on 22 January 2004 and 25 February 2004, Hatang took issue with several aspects of Porogo's response. In brief, he argued that the status of the CDRC and IRC was not clear in relation to the request made and the decisions taken by Porogo concerning the documents. SAHA felt that Porogo had not exercised his mind independently. Moreover, it was unacceptable to make available photocopies of the documents when SAHA's application was to inspect the records themselves. Not having access to the original documents made it impossible to verify their integrity.

Hatang also argued that there were several administrative errors in Porogo's response. For example, Porogo had stated that the applicant was entitled to access certain documents which were in fact not provided. Hatang also refused to accept that certain records, such as the 'Progress report on the work of the TRC Investigation Unit', were likely to contain confidential third party information, as Porogo had contended. He also rejected the contention that certain files were being withheld on the basis that 'family members' of persons named in those documents had to be consulted, as this was not provided for in the Act. Similarly the Act did not allow information to be withheld on the grounds of preventing the embarrassment of a foreigner, which was the reason given for masking sections of an Afrikaans document entitled 'Final report: USA Dollars advance payment'. Lastly, a large number of documents had been withheld on the grounds that they contained third party information, whereas the Act required that, before making

a final decision, third parties had to be *informed,* not consulted, which was the DOJ's interpretation.

LESSONS FROM THE CASE STUDY

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 which deserves to be thoroughly analysed. It goes to the heart of interpretation of the PAIA, and how polarised such interpretations can be. It also raises the question of how committed the intelligence services really are to transparency. Even though the high court applications and counter-applications were between the DOJ and SAHA, the Ministry for Intelligence Services was a looming, if not highly instrumental, presence in the course of events, largely because the records in question had emanated, at least in part, from the apartheid security apparatus.

One issue was whether the ministry had acted lawfully and in the public interest in withholding the records from SAHA, and whether it actually had the prerogative to decide what to do with the records. NIA's response to SAHA's initial 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 and the NIA, or a deliberate attempt to mislead SAHA.

The timing of its establishment, and the inclusion in its brief of how to handle the sensitive TRC records, creates the impression that the CDRC initiated by the intelligence minister intruded on the mandate and to a certain extent usurped the role of the DOJ.

Another issue that requires scrutiny is the IRC's composition, method, and recommendations. Although 'trained' for its task, the committee consisted of middle-ranking officials who were given considerable power to recommend the 'reclassification' of documents, some of which had previously not been classified at all. Moreover, the IRC made its recommendation to the CDRC, which consisted of academics and government officials.

Also questionable is whether the IRC had adequate expertise, especially in view of the administrative errors and high incidence of legally unsound reasons given for withholding, masking or refusing to disclose documents. It appears that the Protection of Information Act may have unduly influenced the reasons given for refusing access to some records.

Although, in an interview, Porogo insisted that the DOJ exercised independent judgment in deciding how to respond to the SAHA request, the deliberations and recommendations of the IRC certainly had a trickle-down effect, and affected

the DOJ's response to the SAHA request rather than being guided solely by the PAIA provisions. In an interview, Raswiswi defended her department, arguing that the DOJ's director-general had studied the request and taken different decisions to those recommended by the IRC. However, there was clearly considerable role confusion, as SAHA argued after receiving a copy of a confidential worksheet from the IRC, which needed further clarification over why certain documents were not disclosed or only partially disclosed.

Another problem was that the minister of justice decided to accept records regarded by Dr Minyuku as 'sensitive', and hold them for safekeeping at the ministry for intelligence services. Minyuku probably thought he was acting correctly, and even in the national interest. However, the effectiveness of these actions is questionable, as many of the documents were in the public domain, while copies of others were probably in the hands of individual researchers and investigators. The minister's decision to hold the documents for 'safekeeping', rather than deal with them expeditiously (for example, by passing those that needed further investigation onto the law enforcement authorities), raised issues about their integrity, and suspicions about the intelligence services' motives.

The matter of the 'sensitive TRC records' was only resolved after many months and much wrangling between the applicant and respondents' lawyers. It was settled out of court. The saga suggests that the post-apartheid intelligence services are ambivalent about disclosures of the past. According to Dennis, during the TRC hearings SASS had been in favour of disclosing past secrets, especially those relating to South Africa's chemical and biological warfare programme, but senior former NIS officials had resisted the idea (interview, 25.07.05).

Throughout the dispute about the whereabouts of the TRC documents, the cabinet remained silent, which suggested that it supported – at least tacitly – the way in which then ministers concerned had handled the affair.

Some of the records related to members of the ruling ANC, and there was speculation that the withholding of the records and the claim that the list of informers had never existed was an attempt to hide information about the ruling party and its members from the public. PAIA regulates access to information held by public or private bodies irrespective of the origins of those records. When deciding to grant access, the only relevant factor is whether one of the grounds for refusal applies. While the minister for intelligence services may have been concerned about certain information being released into the public domain, a more appropriate response would have been to develop clearer policy guidelines on how to handle requests for information that originate from political organisations.

According to Raswiswi, the department later received other requests for

TRC-related documentation. One of these involved documents about the deaths of four anti-apartheid activists in the Eastern Cape known as the 'Cradock Four' who were killed by apartheid security policemen in the mid-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 (interview, 4.08.05).

SAHA's request for access to information about the TRC must be seen in the context of the TRC's experience of trying to uncover the apartheid-era records of the security establishment. During its investigation of apartheid-era records, the TRC found that there had been a massive destruction of records by the state's intelligence agencies (primarily the NIS). Alarmingly, the destruction of records continued even after a democratic government had taken office, until the cabinet imposed a moratorium on this practice in 1996.

It is cause for concern that, when SAHA lodged its requests, no clear guidelines existed for handling requests for access to TRC documents. While the DOJ stated that it dealt with requests for access within the PAIA framework, SAHA implied that the provisions of the Protection of Information Act had influenced the DOJ's decisions – which the services denied.

APPLICATION FOR RECORDS RELATING TO THE STRATEGIC ARMS PROCUREMENT PACKAGE

The second case study is that of *CCII Systems (Pty) Ltd vs M P G Lekota*, heard in the High Court (Transvaal Provincial Division) by Justice Southwood in 2002. CCII sought an order to direct the respondent, Mosiuoa Lekota, then Minister of Defence, to furnish certain records pertaining to the subsystems to be installed on corvettes ordered by the 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 subsystems 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 decided to purchase various new weapons systems for the SANDF. These included four patrol corvettes for the South African Navy. Each corvette consisted of a hull, propulsion system, and

combat suite. The DOD and Armscor 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 believed that the tender process had been unprocedural, and it therefore sought access to the records arising out of the tender process (interview with Wayne Hendricks, 28 July 2005).

On 15 January 2002 the applicant had made a PAIA request to the DOD for records 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. (In his eventual judgment, Judge Southwood noted that the applicant did not question the legality of his requests being considered by the Information Committee, and therefore did not take issue with this factor.)

In the remaining cases, the DOD claimed that the documents either did not exist, or refused to give access to them, citing grounds provided for in 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 PAIA which requires that when a request 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 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.

In his judgment, Judge Southwood emphasised 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 PAIA 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 that 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 2002).

Judge Southwood went on to consider the merits of the legal arguments presented by the applicant and the respondent. Those arguments and aspects of the judgment 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) of PAIA, which protects commercial information of a third party, and section 37(1), which protects confidential information of a third party. In Southwood's view, 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 that could be severed (deleted) because of their sensitive contents, so as to make the rest of the document available to the applicant.

In papers 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 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 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 that 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 (quoted in Southwood 2002)

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 could be invoked for 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 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 four years had elapsed since the contract had been awarded, and the information was therefore merely of historical interest. In any event, the respondent had failed to provide information which 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 an adequate reason 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 DOD; and all correspondence concerning these matters between the DOD and the German Frigate Consortium (Southwood 2002).

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 had argued 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 was untrustworthy, nor that the information made available to him would be at risk.

He also rejected two other reasons provided by the respondent. The first was that that the request was vague and unspecified (section 45(b) of PAIA). This reason was provided in relation to the request for all internal correspondence and memoranda concerning 'these matters' with the DOD. 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 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 holds important lessons for the intelligence services, because it too relates to information regarded as protected in terms of PAIA, yet found to be releasable in the Southwood judgment. The judgment therefore sets precedents that will have to be taken into account by all public bodies.

It highlights the need for bodies considering requests 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 should 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 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 contextualised and properly motivated, and 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. Southwood noted that not only is the ground for refusal a discretionary one, but that the case for non-disclosure would have to be motivated.

He also 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*, he 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 judgment suggests 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. Raising additional grounds for refusal, particularly the grounds that disclosure could prejudice the defence and security of the Republic, provoked a cynical response from the judge, who went on to order disclosure.

The Southwood judgment can be regarded as a very strict interpretation of 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 judge's findings, despite the self-imposed strictures of secrecy and confidentiality it assumed were sufficient to shield records that it held from disclosure to a requester.

THE HEFER COMMISSION

In 2003 President Thabo Mbeki appointed a judicial commission, the Hefer Commission, to assess the claim made by a former anti-apartheid activist and intelligence operative, Moe Shaik, supported by the ANC veteran Mac Maharaj, that the serving national director of public prosecutions (NDPP), Bulelani Ngcuka, has been an apartheid-era spy. The allegations were politically explosive, particularly because Shaik and Maharaj were seen as politically supportive of the deputy president, Jacob Zuma. Tension between Mbeki and Zuma was starting to show. Zuma had drawn the attention of Ngcuka because of his relationship with the businessman Schabir Shaik, Moe Shaik's brother, who was also being investigated by the public prosecutor. The claims against Ngcuka created a political uproar, and generated intense media interest.

The hearings of the commission were held publicly. Judge Hefer duly summoned the intelligence services to confirm whether the allegations were true. The intelligence services – both the NIA and the SAPS – decided to refuse to reveal the contents of their records to the judge, on the grounds that these were classified secret. They argued that the law, in any case, prevented them from disclosing the identities of intelligence 'sources', and pointed out that Mbeki could have direct access to the intelligence that might assist to answer the question the judge was meant to investigate, if he so wished.

Shaik and Maharaj were left to produce and present to the Commission copies of the record they said were the basis of their claims – which the Minister of Intelligence Services later demanded be handed over to the intelligence services even if they were only copies. In the end, all that Judge Hefer could report was that

Ngcuka had 'probably not' been an apartheid-era spy, further making the point that he could not be conclusive because he did not have access to the intelligence records that might have assisted him to make a determination of this matter.

The Minister for Intelligence Services, Lindiwe Sisulu, commissioned a review of the saga following these developments. It was chaired by Professor Norman Levy, a seasoned academic. Serving with him were a lawyer, Christine Qunta; a legal academic, Professor Nico Steytler; a sociologist, Professor Paulus Zulu; and a media expert, Professor Guy Berger. They were assisted by several senior managers from the intelligence services, and the project was conducted under the auspices of SANAI, the training facility for the intelligence services. The review committee did not pronounce on the merits of the judgment or even deliberate very directly on how the proceedings had been conducted. Instead, a number of broad, policy-related problems were extrapolated and formed the basis of the report submitted to the Minister.

Firstly, the report addressed in philosophical terms the challenges of managing the tensions between the public's right of access to information and the intelligence services' right to withhold information. Levy (2004) argued that the existence of the services was a constitutional requirement, and that they had a duty to preserve secrecy, and to protect from disclosure, sensitive information in their possession. Steytler (2004) also recognised that the South African intelligence services are faced with the challenge of balancing the requirements of the constitution with their legally defined role and methods permitted in law. He explored 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. He ended his analysis on the optimistic note that leveraging the right vehicles, possibly in combination with each other, can yield a result that upholds the principle of access to information.

Qunta (2004) pointed to legal precedence, both locally and internationally, which held up the principle of protecting the identities of sources, at least in police investigations. However, Zulu (2004) reminded the Minister and other readers of the report 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 United States and United Kingdom to go to war against Iraq.

The study concludes on an optimistic if ambivalent note, arguing strongly in favour of transparency by the intelligence services, yet sympathising with the notion of absolute non-disclosure of the identity of sources. On reflection, the

study authorised by the Minister for Intelligence Services did not really answer the question of how to deal with apartheid-era intelligence records, or even interrogate whether there was an adequate policy and legal framework for this matter. The terms of reference of the Hefer Commission were changed at least once, yet the reviewers did not address the issue of why this was done. Moreover, it remains unclear why Mbeki established a judicial commission when he could as easily have requested a briefing or even an investigation by the intelligence services into the question of whether Ngcuka had been an apartheid-era spy. The plausible answer to that question is that such a process would not have satisfied public interest, since it would have taken place behind closed doors. But detractors accused the President of playing political games in establishing a process which was hamstrung by the very conditions under which it would have to do its work. Judge Hefer expressed frustration that he did not have access to the records that might have assisted him in answering the very question that he was supposed to answer. And once the Commission's findings were announced, Mbeki issued a thinly veiled warning to those who would dare accuse others of being apartheid-era spies never to repeat the misdemeanour.

The question that arises is whether the principle of secrecy of the identity of sources is an immutable principle, even under those circumstances where there is overwhelming public interest in the matter. The ready answer to this question is that the consequences of confirming such an allegation, were it true, would have been to violate the principle of honouring the confidentiality which informants expect when providing information to authorities. That the allegations were made at all by Shaik and Maharaj, and prompted the establishment of a high-level enquiry, suggests that there were unresolved questions about the transition and the records of the past.

CONCLUDING REMARKS

The Ministry for Intelligence Services has played an ambivalent leadership role in respect of the PAIA, appearing at first to support, and even co-ordinate, applications by the NIA and SASS for exemption from the requirements that public bodies produce a manual. The grounds on which the exemption was requested were very vague, and suggested little in-depth policy debate before making the application.

One of the most telling indications of the intelligence services' approach to PAIA came in their response to SAHA's application for access to sensitive records transferred from the TRC to the Minister of Justice, who was also 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 then became embroiled in a long, behind-the-scenes battle to wrest control of the documents from the ministry for intelligence services, in order to process the request.

Had the matter not been settled out of court, it is likely that considerations that were raised in the Southwood judgment would have surfaced. One is that the classification of a record as secret is not a sufficient ground for refusal. The labelling of a document as being secret or top secret has no legal weight; it is a mere administrative measure, at least it was then. The onus remains on requesters to prove that when records are withheld, the reasons comply with the grounds for refusal contained in the PAIA. It is also clear that the Protection of Information Act cannot be used as a basis for refusing access. That Act has its own purpose, namely criminalising the unauthorised disclosure of information, and can only be applied in accordance with its own provisions. In the case of the Hefer Commission, when the intelligence services were called upon to reveal whether Ngcuka had been an agent of an apartheid security service, there appears to have been a lacuna which the presiding judge was unable to fill. Either the legislative framework was inadequate, or the way in which available instruments are utilised is not given due thought and appropriate application by the executive.

The issue of apartheid-era records is very much alive, and in the public consciousness. Most of the requests by individuals, through SAHA, to the NIA were for records about them held by the state. Policy needs to be formulated, and a legal framework established, for dealing with this issue. Ideally, the intelligence services should undertake a proactive declassification process and provide information about the records available to the public, in order to avoid becoming involved in time-consuming searches for records, and possibly expensive litigation over access disputes. There also needs to be a review of the legal basis of the procedures and criteria for classification. The following factors, which are not part of the interdepartmental review process, should be addressed in the regulatory framework: the criteria for classification aligned with PAIA; possible restrictions on who has the authority to classify records; and stricter oversight of classification procedures.

PART THREE

Lessons, conclusions, and policy recommendations

7

COMPARATIVE INTERNATIONAL EXPERIENCES

In the decade after the Cold War, many countries introduced access to information legislation, also commonly referred to as 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. They joined a number of countries that had already enacted such laws, including Sweden (1949), the United States (1966), the Netherlands (1980), Canada (1982) and Australia (1982). This trend has usually reflected a demand for greater accountability on the part of government and other public bodies, especially following crises of confidence related to security issues or foreign relations.

As security and intelligence organisations work largely in secret, studying how access to information legislation impacts on their operations in democracies may be useful for South Africa. Although different parliamentary democracies adopt access to information legislation in response to different historical circumstances and concerns, reflecting on their experiences can cast greater light on the tensions between national security interests on the one hand and the public's right of access to information on the other.

THE UNITED STATES

The United States has a long-established tradition of freedom of information, and is often seen as having many of the answers managing the balance between secrecy and transparency. Yet it is important to remember that freedom of

information in the United States arose out of particular historical conditions, and that many gains are the results of struggles in and outside of the courts.

Origins of the Freedom of Information Act

In 1966, Congress enacted the Freedom of Information Act (FOIA), which introduced a general right of access to public records. This was in response to state departments, which were increasingly resorting to secrecy, often citing Cold War imperatives as justification. Prior to 1966, there was no general right to inspect federal records, although some states had, in differing degrees, introduced various forms of open government. Under a provision of the Administrative Procedure Act, federal records were available to 'persons properly and directly concerned', subject to vague exceptions that were intended to protect the public interest but had no supporting judicial remedy. This provision was ultimately repealed and replaced by the FOIA, as it had in effect become a charter to withhold rather than an instrument of disclosure (Adler, 1991).

The FOIA is better understood in the context of other laws that impact on access to information and balance the interests of the individual. One such law is the Government in the Sunshine Act ('Sunshine Act') of 1976, which was based on the view that the government should conduct the public's business in public. This Act applies to all agencies that are subject to the FOIA, and opens their meetings to the public; it contains exemptions that mirror closely those found in the FOIA. Another law is the Privacy Act of 1974, which reinforces the constitutionally protected right of privacy of American citizens, and includes a system for individuals to access records about themselves (with exceptions). Through this Act, Congress has acknowledged and sought to regulate the practices affecting the right to privacy, such as the collection, use and dissemination of personal information by the federal agencies, made easier by the use of computers and technology.

Main features of the Freedom of Information Act

The FOIA's premise is that, unless exempt from this requirement, all federal government records must be accessible to the public. Any member of the public ('any person') may request a record: the Act does not stipulate a citizenship requirement, and the courts have interpreted the definition to include foreign citizens, corporations and governments. A requester does not have to give a reason for the request. The Act also limits the response times for requests to be attended to, the costs of making requests and an appeals mechanism. In the beginning, some federal agencies resisted the Act and employed a variety of ways to discourage its use, such as 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 various amendments in 1974. In 1976, minor amendments were introduced that dealt with standards for determining more precisely which 'other statutes' could be used as grounds for withholding information.

Further amendments were enacted in 1986, when the United States government was concerned that the Act's exemptions did not adequately protect from disclosure confidential sources, ongoing investigations, certain manuals and other sensitive, non-investigative, law enforcement materials. Thus the amendments included the following exclusions: 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; and classified records of the FBI pertaining to foreign intelligence, counterintelligence or international terrorism (Adler, 1991).

Grounds for refusal (exemptions)

The FOIA, in its current form, provides for the following exemptions: national security information; internal agency rules; information exempted by other statutes; business information; litigation to reverse FOIA; personal privacy; law enforcement records; financial institutions' records, and oil well data. Of particular relevance to intelligence is the first exemption, which states that the FOIA does not apply to matters specifically authorised to be kept secret, in the interest of national defence or foreign policy, under criteria established by an executive order. However, the American security and intelligence services are not excluded from the Act's provisions; indeed they have been the targets of civil rights groups and a massive body of case law has developed around the courts' application of the Act.

The United States makes statutory provision for the protection of classified information. Executive order no. 12356 clarifies which information should be classified. The 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; government programmes for safeguarding nuclear materials or facilities; cryptology; a confidential source; or other categories of information related to the national security that require protection against unauthorised disclosure, as determined by the president, agency heads or other

officials who have been granted original classification authority by the president (Adler, 1991).

Status of CIA files

The American security and intelligence agencies are not, as a class, exempt from the provisions of the FOIA. However, in 1984, Congress amended the National Security Act of 1947 to allow certain 'operational files' of the CIA to be exempt from the search and review requirements of the FOIA (Adler, 1991). Significantly, this amendment was passed with the support of the American Civil Liberties Union, a vocal freedom of information advocacy organisation. Through this statute, Congress hoped to relieve the agency of the frustrating administrative burden of having to search and review certain files that 'almost invariably prove not to be releasable under the FOIA'. And in this way, the statute aims at reducing the processing backlog and delays in responding to FOIA requests, 'while preserving undiminished the amount of meaningful information releasable to the public' and, in addition, keeping CIA sources confidential (Adler, 1991).

'Operational files' included files of the operations, science and technology, and security directorates. The operations directorate's files document the conduct of foreign intelligence or counterintelligence operations, intelligence, security, liaison arrangements, information exchanges with foreign governments or their intelligence or security services. The science and technology directorate's files document foreign intelligence or counterintelligence collection through scientific and technical systems. The security office's files document investigations into the suitability of potential foreign intelligence or counterintelligence sources. Significantly, files that are the sole repository of disseminated intelligence are not regarded as operational files (Adler, 1991).

Impact of freedom of information legislation

Freedom of information has been used extensively in the United States to defend and uphold constitutional rights. In a political environment that has simultaneously addressed the challenges of classification and declassification for which there is also an Executive Order, the intelligence agencies could not afford to be complacent about the issue of access to information. As a consequence, there exists a culture of public information about the workings of the intelligence community, which translates into the many courses offered by universities, academic research, as well as a critical media.

The Commission on Protecting and Reducing Government Secrecy (Moynihan Commission 1997) was established in the mid-1990s, in response to public

concerns about the extent of governmental secrecy. Its 1997 report found that the subjectivity of officials led to inconsistent interpretation and application of the classification and declassification criteria. As this secrecy system had no statutory basis, each time the administration changed, a new classification and declassification executive order was issued. The commission found that these regular amendments disrupted the efficient administration of the classification system. Dissenting public officials quite often simply dragged their feet on implementing policy changes, knowing full well that the appointment of the next administration would bring yet another change. The commission also expressed concern over the reliance on the Freedom of Information Act as an instrument for declassification. The FOIA is limited, as it only applied to individuals making requests. This naturally makes it difficult for interested parties to make requests about secrets to agencies. The agencies are at an advantage, as they can choose to cut out substantial chunks of information, which might have provided the requester with significant contextual information. Concerned that a culture of openness would never develop unless a culture of secrecy is restrained, the commission recommended mechanisms for the proactive declassification of intelligence records and oversight structures to ensure compliance with this process (Moynihan Commission, 1997).

The United States' intelligence services are subject to extensive and public scrutiny, which ensures a significant degree of transparency about them. Over the years, 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.

CANADA

In Canada, two pieces of complementary and mutually balancing legislation deal with freedom of information: the Access to Information Act of 1982 and the Privacy Act, 1982.

Origins of the Access to Information Act

The Trudeau government introduced this legislation at a time when Canada was undergoing substantial constitutional reform. The McDonald Commission had been set up to investigate abuses in the Royal Canadian Mounted Police (RCMP), amid growing controversy over the role of the security forces. The result was the

establishment of a civilian intelligence agency, the Canadian Security Intelligence Service (CSIS), in 1984.

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

Main features of the Act

The Access to Information Act of 1982 promotes the following principles: government information being made available to the public; limited and specific exceptions to the right of access; and independent (of government) reviews of disclosure decisions. In Canada, the Act's use is restricted to citizens and permanent residents or persons present in Canada, thereby excluding foreigners. As in the USA, the security and intelligence agencies are not excluded from the ambit of the Act.

In compliance with the requirement to publish categories of information held, the CSIS lists the following: communications security; planning and co-ordination of activities; counter-intelligence and counter-terrorism; access and disclosure procedures and requests; personnel records; internal security of the Service; scientific, operational and technical support; supply of security assessments to other government departments; and policy, administration and management of operations involving human sources (Hazell, 1989).

Under the Act, a public body must disclose a record if there is such a request. However, the general principles are that a government body is not obliged to create a record that does not exist. CSIS receives requests from a wide range of sources including historians, many of whom admit to submitting similar requests to several agencies in the hope of getting as comprehensive an answer as possible. Part of the reason for this is that the CSIS frequently uses the provision in the Act that allows them 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.

In the Canadian Act, the following kinds of information are protected from disclosure: information relating to 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's diverse system of controls over the security and intelligence community provides a fair measure of public accountability in this area of governance.

Following recommendations by the McDonald Commission, an independent body was established to review the functioning of the CSIS: the Security Intelligence Review Committee (SIRC), whose members 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's four main functions are to: review CSIS's performance of its duties; investigate complaints of any persons against the CSIS; investigate complaints about security clearances; and review cases concerning national security matters. SIRC releases an annual report to the public about its work, and generally has the confidence of the public (Rankin, 1986). Another mechanism of control is the Inspector-General, appointed by the cabinet. Like the SIRC, the Inspector-General has wide access to CSIS documentation, except for cabinet records. In Canada, ministerial responsibility lies with the solicitor-general, to whom the CSIS, the Inspector-General and the SIRC all report (Rankin, 1986).

Canada, like many other countries, learned the lesson of allowing the security services to function under conditions of unaccountability. The legislative measures put in place are impressive but not without problems. However, Canada is a useful comparison for South Africa, which has adopted many features of the legislation dealing with access and the functioning of its domestic security service, which in many respects can be equated to South Africa's NIA.

INDIA

Like South Africa, India is an established democracy that is beset with problems: a colonial legacy, including a Westminster system of government, and the vestiges of many British dominion laws; an economically stratified society, of deep social, religious and caste divisions; and a volatile political climate. Even with these problems, India remains one of the world's largest parliamentary democracies. Bordered by 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 scores of civilian lives. Despite these conditions, the right to information has been a concern throughout the decades of freedom.

Origins of the Right to Information Act

For several years, the Indian government had been under pressure to introduce access to information legislation, and eventually introduced a bill at federal level in 1999. The genesis of the right to information dates back to 1975 when, in the

case of *State of Uttar Pradesh v Raj Narayan*, the Supreme Court of India acknowledged that, although not specified in the constitution, the right to information was implied in the right to freedom of speech and conscience. The Supreme Court later ruled (in 1982), in the case of *SP Gupta v President of India*, that access to government information was an essential part of the fundamental right to freedom of speech and expression, stating:

> 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. (Martin & Feldman, 1998)

In 1997, the Indian government established a working group to draft a bill that 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 the government's intention to introduce the Freedom of Information Bill.

The bill was strongly resisted, particularly by public officials (India Together, 2006), and the version passed in 2000 was discredited as a half-hearted commitment to freedom of information. The bill was withdrawn shortly afterwards and replaced by a version that satisfied at least some of the critics' concerns.

Legislative framework for the intelligence services

India's strained relations with its neighbours have resulted in the country adopting a defensive security stance. National security is seen to require strong intelligence and defence capabilities to protect territorial integrity; and strong police and domestic security capacities, to counter perceived domestic security threats. There is, in a sense, continuity in the aims of the security institutions: under British rule, they protected British interests; on attaining independence, they were converted to serve the interests of the ruling elite and found themselves increasingly at odds with marginalised political groups (Subrahmanyam 2000).

In India, the organisation and responsibilities the intelligence services are not established or regulated by legislative parliamentary acts. And it is against this background that the application of freedom of information legislation must be

seen. Nonetheless, public access is affected by the many laws regulating public safety and national security: 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 Act

One of the legacies of British rule was the Official Secrets Act of 1923, which made the disclosure of classified information in India a criminal offence. The Act was based on the UK Official Secrets Act. In the motivation for the Freedom of Information Bill, it was said that, once passed by parliament, it would take precedence over the Official Secrets Act and be only for the use of Indian citizens. The bill would be applicable to all federal public authorities and require them to maintain records, which would be subject to disclosure on request. The bill required public authorities to appoint public information officers, and assist persons wishing to access information, Recognising the unequal levels of literacy, this assistance was to include translating verbal requests into written form. The bill also provided for an internal appeal to a designated individual or office within the public body to which the original request was made, in the event of a refusal. The federal bill was finally passed as the Right to Information Act, and became operational on 12 October 2005 (India Together, 2006).

Exclusions and exemptions

Article 16 of the bill provided for a blanket exclusion of all intelligence and security organisations listed in the schedule, which the central government may amend by notification. Not surprisingly, the legislation adopted by states included exclusions that were aligned to the national Act. Rajasthan was one of the first states to introduce freedom of information legislation. In section five of the Rajasthan Right to Information Act, the grounds for refusal apply to 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 organisations; the conduct of centre-state relations, including information exchanged in confidence between the central and state government or any of their authorities/agencies; 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.

In summary, the introduction of freedom of information legislation was a positive step for India, although the categorical exclusion of the intelligence services from the bill suggests that the public will continue to be afforded little official information about their functioning.

LESSONS FOR SOUTH AFRICA

South Africa can derive many lessons from studying the access to information legislation in other countries and its relevance to the intelligence services.

In some countries (for example India), the security and intelligence agencies are specifically excluded from the access to information legislation. However, in other countries, such as the United States and Canada, the intelligence agencies are subject to freedom of information legislation.

The one common area is the range of exceptions. Generally, the following categories of information are exempt from disclosure: private information about individuals; information relating to defence, security, and international relations; information about ongoing investigations in the law enforcement sector; commercial and economic information; and operational procedures of public bodies. In relation to intelligence, the scope covers the identities of sources and intelligence officers. Thus, provision is made to protect information held by the intelligence services, even when they are subject to the access to information legislation.

Official secrets legislation or regulations generally co-exist with freedom of information legislation. The introduction of the latter has certainly not sounded the death knell for official secrecy. Indeed the state's right of refusal to disclose security and defence information seems to be an inalienable given, which makes the need for managing classification and declassification of information especially relevant.

Some countries have introduced separate legislation to protect the privacy of the individual, to ensure that persons have access to information about themselves, and that such information may not be disclosed to unauthorised persons. However, such legislation usually excludes 'national security' information.

In other aspects there is little uniformity. Certain countries have a well-established body of judicial precedence, as in the case with the United States, while others do not, which is the case with Canada. Nevertheless, in many cases, the trend is to link access to information legislation with other oversight mechanisms, such as parliamentary oversight bodies (in Canada's case, a privy council) and inspectors-general reporting to a minister or the legislature.

Despite the above similarities, it is necessary to be circumspect in deriving lessons from the example of other countries. While belonging to the body of countries that has adopted freedom of information legislation, South Africa has done so under specific circumstances, in response to particular pressures, and at a certain level of maturity and stage of evolution.

Managing records from the past

Apart from access to information legislation and how countries' intelligence services may be subject to it, there may be value in reflecting on how societies in transition manage their records. In South Africa, the issue of whether a separate regulatory regime is required for the handling of such record appeared to have been unresolved when the Hefer Commission sat.

The example of former communist countries in handling records of the state security apparatuses is sometimes referred to. After the collapse of the Berlin Wall and the East German state, the new integrated German state acted quickly to take control of the records of former communist state, and went as far as publishing legislation that regulated access to and the utilisation of security service records. The *Act Regarding the Records of the State Security Service of the Former German Democratic Republic (Stasi Records Act)* was passed in December 1991. It aimed to facilitate individual access to personal data which the State Security Service had stored on individuals, to protect the privacy of individuals, to promote the 'historical, political and juridical reappraisal of the activities of the State Security Service' and to provide public and private bodies with access to the information required to achieve the purposes of the act (section 1, Stasi Records Act 1991).

The act is detailed and prescriptive about the use of the records, and directs the conditions under which particular categories of records should be directed to particular agencies, when they may be used for criminal proceedings, and the conditions under which access to personal records may be given. It also carefully details which records are subject to the Act, and which are not.

The act is also very particular about procedure. All requests for access to the relevant records of the former Stasi must be made in writing, and a requester must properly identify himself or herself. Particular care is exercised in determining what access is given. In Part 3 of the Act (Use of the State Security Service Records), it is specified that where a person has requested information pertaining to records about himself for herself, if information about third parties might be disclosed through the inspection of such access to a record, these third parties must give their consent. Access can be granted if 'separation of personal data regarding other data subjects or third parties is not possible or is possible only

with unreasonable effort, and there is no reason to assume that the other data subjects or third parties have an overriding legitimate interest in keeping them secret' (section 12, 4.2.).

The person responsible for the execution of the Act is a Federal Commission, responsible to the Interior Minister. The powers of the Commissioner are spelt out in law, as are the measures that must be taken by the incumbent to ensure the safety, integrity and security of the records. The Federal Minister is assisted by a statutory Advisory Commission.

The Stasi Records Act has a whole section dealing with data subjects and third parties (section 13), 'data subjects' being persons about whom the State Security Service collected personal data by deliberate, including secret, information-gathering or spying. As a rule, data subject enjoy the right of access to information to records about them. In their requests, they would be expected to supply particulars which make it possible to locate the records, but 'the purpose for which the information is requested need not be given' (s.13.1). The act is strongly weighted in favour of data subjects', to the extent of exposing those who have collected or provided the information that made its way to the police. Section 13.5 states:

> If code names of employees of the State Security Service who gathered or evaluated personal data regarding the data subject, or names of their officers, together with particulars which make it possible to positively identify these employees, can be found in the existing prepared records which the data subject has inspected or for which he obtains duplicates, the names of such employees shall be provided to the subject at his request. Section 1 shall also apply to other persons who informed on the data subject in writing, if the contents of their reports were written in such a way as to be detrimental to the data subject. The interests of employees and informers in keeping their names secret shall not rule out disclosure of their names.

Of interest is the provision that the above clause would not apply to 'employees of the State Security Service if they were not at least 18 years old at the time of the activities in question' (s.13.6). This raises the disturbing prospect that some of the employees of the State Security Service were in fact mere children.

Similar provisions to those found in the Stasi Act are to be found in Hungarian law, which also has a special legislative dispensation for records of the former Security Services. The law has been reviewed several times over the past decade and today is part of a body of law relating to the organisation of the intelligence services, the protection of individual privacy, and the management of public records. The act dealing with security records of the past is Act No. 111 of 2003

On the Disclosure of the Secret Service Activities of the Communist Regime and on the Establishment of the Historical Archives of the Hungarian State Security. Records covered by the act cover the period 21 December 1944 to 14 February 1990. In similar vein to the Stasi Act, the categories of both those who informed and those who were the targets of intelligence collection are defined. The Act then stipulates the procedures for the handling of such records, and the conditions under which they may be accessed.

The Hungarian law appears to differ substantively in its handling of the secrecy of identities of informers, from the Stasi Act. This is done through the classification status accorded such records. Article 2 .1 of the act reads thus:

> The previous security status of the data to be found in the documents falling under the effect of the Act shall cease to exist by virtue of this Act, except if the classification of the data is maintained by the person entitled thereto.

This apparently under the Secrecy Act of 1995. Moreover, the security status of the data which is subject to the act, and which is classified as secret under the Secrecy Act, may be maintained if it applies to a person who was attached to the staff of the national security services in the period 15 February 1990 and 26 May 2002, or to someone who secretly cooperated with the services. The secret status can also be maintained if it applies to a person whose activities or identity, if exposed, might become the victim of a crime seriously violating or endangering his or her life, health or personal freedom, or that of his or her relatives (Article 2.2). In general there is a more cautious approach to disclosure even of the former security service records, and due regard is also given to what is considered to be in Hungary's national interest.

The handling of records of the former security services

Both the Stasi and Hungarian experiences demonstrate important aspects that should be considered when dealing with records of former security services of authoritarian societies. In such cases, as was the case in South Africa, there is a desire to get to the bottom of the state secrets, particularly the role of the security services in upholding the regime. In the South African case, the TRC was one of the main vehicles that addressed this need. However, the Act establishing the TRC, the *Promotion of National Unity and* Reconciliation *Act, 1995,* did not make specific provision for the handling of records of the former security services, in the way that the above mentioned Acts did. The TRC did have the power to demand records and to issue subpoenas, and in the course of its investigations, it had powers of search and seizure, but there was not and to this date is not a specific South

African law dealing with the management of the records of the former security and intelligence services.

The consequence has been a chaotic state of affairs. It should be of concern that apartheid era security establishment records remain dispersed throughout the structures of the present security establishment, with differing standards of care and custodianship. A good example of such records being well managed is those under the control of the SANDF. In other cases, for example, surviving Security Police files which were located, secured and listed under TRC direction in 1997/8, were several years later in chaos (interview with Verne Harris, 1 September 2003).

A further problem has been the illegal removal of records by former members of the security establishment. Other records that found themselves in the hands of the TRC were not properly retrieved and handled when the TRC concluded its work. The records of the Bantustan security services have also been compromised, having been taken up in a haphazard way by the different public service and security sector institutions. The systematic destruction of records, which apparently continued even after a democratic government had been installed, was the direct result of not having a specific policy position on what to do with such records.

Anecdotal recollections by members of the security services suggest that the former regime and the liberation movements felt as they were negotiating a common future, that the past was best left to rest, and that there should be no exposure of the other's spies, because this might have caused embarrassment or even put the lives of collaborators at risk. The situation that came to obtain then was that persons, who had been spied upon by the apartheid security forces, were never to know who had betrayed them. And persons who defied the law in giving state secrets to the enemy (many of them in the ranks of the security police and military intelligence), were given the uneasy assurance that the risks they took would not be exposed. In this context, though and without the protection of an adequate policy and legal framework that deliberately balances the right to know, with the right to protect, and takes into account other imperatives such as the right to justice, the accusations of treachery linger, causing the kind of national crisis that the claims against Ngcuka that the Hefer Commission was required to resolve. It may be that South Africa still needs to explore such a policy and legislative framework, to forever put the apartheid ghosts to rest.

8

CONCLUSION AND POLICY RECOMMENDATIONS

The primary aim of this book has been to explore a possible policy framework for determining what information about the intelligence services, or information held by them, should be made available to the public. The route has been circuitous, covering the history of official secrecy, the transition to democracy, and some international comparisons. Although the focus has been on the policy for implementing PAIA, the research has raised broader issues of public accountability, governance, and democratic control of the intelligence services. What has become evident are the multiple means of accessing information about the post-apartheid intelligence services. Therefore, some of the strengths, weaknesses, and efficacy of different ways of accessing this information have also been assessed.

The secrecy under which intelligence services conduct their business is a worldwide phenomenon, and a feature of both authoritarian and democratic political systems. Since the end of the Cold War, global conflict and internal instability have persisted despite the introduction of the concept of 'human security'. Debates about national security and the governance of the security sector have raised important issues, both internationally and in the developing world.

States continue to justify using extraordinary regulatory measures not only when there are real and grave threats to life and limb, but under many guises labelled as the 'national interest'. Resorting to secrecy is an example of such an extraordinary measure. By and large, placing issues in the security realm signals a failure to address them through the normal rules of political engagement. A resort to secrecy by the state (particularly if this is excessive) indicates that the normal

course of politics has failed, and that society is being driven back into the abyss of unaccountable and authoritarian state conduct.

Deciding when official secrecy has become excessive is a problem confronting all democratic societies. Before 1994, secrecy in South Africa was an integral part of an undemocratic, racially exclusive constitutional order that undermined human rights. In post-apartheid South Africa the intelligence services are still claiming a right to secrecy, because of continued threats to national security and because they have a constitutional duty to protect state secrets, alongside their duty to contribute to state transparency. Striking a balance between secrecy and transparency is a continuing challenge which, during the first ten years of democracy, was not helped by the executive's inability to formulate a comprehensive and viable policy framework reconciling the constitutional imperatives of access to information with the intelligence services' legitimate constitutional role. The fact that the legal framework remains incomplete and contradictory is evidence of this failure.

MANAGING INTELLIGENCE INFORMATION IN THE TRANSITION

The legal framework that has historically covered state information has been problematic and does not fit in the post-1994 context. From 1912 onwards South Africa was subject to the Official Secrets Act, which was modelled on British legislation and provided for severe penalties for disclosing state secrets. This was followed by the Protection of Information Act of 1982, which reinforced the culture of penalties for the disclosure of secrets. A debate about governmental accountability is needed if a balanced approach to classification of official information is to emerge. Issues to be addressed include who defines what is legitimately withheld as secret or confidential; what checks and balances exist to ensure that officials exercise diligence in their management of information; and how members of the public can be sufficiently informed and reassured that government is acting in their best interests.

In South Africa, the entrenchment of democratic principles in the new political dispensation created the basis of a new culture of accountability and transparency in the intelligence services. While all the old legislation establishing the apartheid intelligence organs has been repealed, and new laws made to establish and regulate the new intelligence services, there is still a significant continuity with the old order. In terms of the transitional agreements, the administrative systems and regulations of the NIS were to have been used for a short period of time and then revised. In reality, the review has been very slow, with the result that the new

services are still operating under the arcane regulations and systems inherited from the old order.

Vestiges of the old political order, the law and administrative instruments designed to protect classified information rest uneasily with the new constitutional right of access to information. These relics include the Protection of Information Act of 1982 and the MISS, a cabinet directive that gives officials the authority to classify documents on the grounds of protecting national security, and thus restrict public access to the information contained in the documents. The MISS is a post-1994 initiative, but is based on an administrative instrument inherited from the apartheid era.

THE MERITS AND DEMERITS OF SECRECY

In South Africa, the implications of the constitutional right of access to information have been studied in areas such as employer-employee relations, health, trade practices, criminal investigations, and trade matters. Emerging from a number of conceptual analyses (Bok 1978, 1982; Mathews 1978; Robertson 1999), several issues help to put the policy options in perspective. A central question is whether a value judgment can be attached to secrecy or transparency, and whether either can be regarded as good or bad for governance, especially of the intelligence services. While this is a complex issue, these authors make an overwhelming case for more, rather than less, transparency, especially on the part of public agencies.

A cynical view is that access to information legislation does not necessarily facilitate open government, because the onus is on the public to ask for information rather than on the government disclosing it. Such legislation could be seen as little more than a revised system of information management, which continues to favour the elites, especially as such legislation rarely offers access to vital information about policy-making, and is weighted in favour of facilitating access to personal files.

These misgivings need to be placed in context. In societies with no access to public records, and where that space is filled with repression, winning the right of access to information is a momentous victory. One example is South Africa, where access to information is entrenched in the constitution as a fundamental right. Moreover, the legislation detailing the exercise of this right – the PAIA – promotes a culture of transparency by providing for the voluntary disclosure of state information. The issue is whether public bodies are doing enough to promote knowledge about their mandates and functioning. Do they rely exclusively on administering the access to information legislation to satisfy public curiosity or

demands for information? Is there enough pressure on public bodies to produce and disseminate the manuals that play such an important role? Or should they spread knowledge and information in other, perhaps more appropriate, forms? What is true is that access to information legislation alone will not deliver open, transparent, and accountable government, and so other governance mechanisms to promote accountability should not be abandoned.

Another concern is how official records are handled in times of transition, and under conditions of political normality. During periods of transition, the archival record is highly contested: one group seeks access in order to confirm its fears of the worst excesses, while the other seeks to destroy and eradicate evidence of its shameful past. Yet the archival record represents only officialdom's version of reality. The intelligence services will only record what the state perceives as a threat to security, to the likely exclusion of the people's own perceptions of threats to their well-being and security. Of equal concern is that records are often only accessible to the public official or researchers who know of their existence, and are inaccessible to the public. This is precisely why public declarations of the information held by the state, and conditions for easy retrieval and access to such records, become so important. The argument is compelling for intelligence records to be available for scrutiny so that they can never again be erased from memory, as they were under apartheid, or tampered with in order to distort the account of history.

IMPLEMENTATION OF THE PAIA

A lack of state capacity has seriously hampered PAIA's implementation. In fact, its use has largely been confined to organised NGOs, at some cost to themselves. The public seems to know little about the Act, 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.

The attitude of the intelligence services towards the disclosure of information is generally positive, as shown by their voluntary publication of information through promotional material, websites, and responses to public queries via the media and in parliament. However, the heads of the services argue that they have a duty to protect the identities of their members and sources of information, and the operational methods they employ, citing the Intelligence Services Act of 2002 as justification. A review of the Hefer Commission has shown that the law does indeed place such a responsibility on the shoulders of the intelligence services heads, which, according to international experience, is not unusual. It has also shown that, in future, strategies consistent with all constitutional aspects of the

law will have to be evolved to deal with such scenarios. Mandates would have to be exercised creatively to prevent any undermining of the intelligence services' mandates or accountability to the public.

Cabinet and ministerial leadership of the intelligence services, particularly in respect of their implementation of PAIA, has been weak and inconsistent. A greater cause for concern is the fact that oversight bodies – the JSCI, the Inspector-General, and the Human Rights Commission – have also not placed pressure on the services to improve their compliance with the Act. By 2005 SASS had not even appointed a DIO, as required by law, and both the NIA and SASA had, with ministerial consent, applied for exemption from the section 14 requirement to approve a manual. The exemption expired in 2008, yet these services do not appear to have made any attempt to consider what information should be contained in a manual, or to make a case for extending their exclusion.

NIA has been under greater pressure than SASS to respond to requests for information. Most of the requests have been for access to personal information files, and have been granted. However, the lack of adequate resources, mainly properly trained personnel, has resulted in delays in responding to some requests.

The case of the TRC records goes to the heart of how committed the intelligence services are to transparency, and whether they are prepared to uphold the rule of law in implementing secrecy measures. This incident also demonstrates that the issue of apartheid era records is still very much alive and in the public consciousness. The ministry's refusal to admit openly to knowing the whereabouts of the requested records sounds disturbingly like dissemblance. A year after the SAHA lodged an access to information request, it appeared that the records had been in the ministry all along. SAHA was unhappy with the grounds for refusal given in some cases, arguing that they were not covered by provisions in PAIA, but were more in line with the Protection of Information Act of 1982. Moreover, SAHA claimed that the ministry for intelligence had influenced the DOJ's response to the request.

The South African intelligence services cannot escape their constitutional obligations, which is to provide the public with access to information about their role and some aspects of their functioning. The compelling historical basis for this is the role played by the intelligence services at the height of the apartheid era in upholding that system. The cloak of secrecy under which the security establishment functioned contributed to the assassination, harassment, and detention without trial of scores of South Africans. It would be in the public interest for the intelligence services to engage in maximum disclosure. A number of options

not previously considered by the services should be considered. One would be to institutionalise the production of their public annual reports.

PAIA should be reviewed in order to ascertain what state records really need to be protected against unauthorised access and disclosure. In this respect, attention should be paid to the volumes of information already in the public domain, through research, the print and electronic and digital media; it makes no sense for intelligence services to attempt to classify readily available information. Clarifying precisely what interests are under threat would help to address the uncertainty surrounding what information should be disclosed and what information protected.

OTHER COUNTRIES' EXPERIENCES

The records of the former security services are an aspect of what must be managed in societies undergoing transitions to democratic forms of government. In South Africa this was exemplified by the TRC, which uncovered the mass destruction of tons of documents by the authorities in the last years of apartheid. This suggests 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 have also revealed evidence of records being destroyed. In some instances, information was obtained through access to a third country's records, which truth commissions could use to understand the security forces' role. In Guatemala, for example, the truth commission successfully petitioned the American government for access to records that would shed light on its relationship with the regime 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.

Comparing and contrasting the experiences of other countries with access to information legislation is also useful. The principles of access to information are found more or less universally in democracies, and are based on the understanding that citizens in particular have a 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 disclose information voluntarily, rather than rely on requests for access;

- a limitation on grounds for refusing requests for information; and
- an inexpensive and accessible system for processing requests.

Grounds for refusing access to information were also very similar, and included 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, and information relating to policy in the making. All these grounds for refusal, which are applicable in South Africa, are contained in the access to information legislation of the United States, Canada and India, the countries used for comparison.

No single formula for balancing secrecy and transparency was found when contrasting the experience of transparency and access to information in post-apartheid South Africa with that of other countries. Not all intelligence services are subject to access to information legislation: in India, the intelligence services are expressly exempt from their country's access to information laws. This complete exemption, incidentally, also applies to Australia, despite its strongly rooted culture of access to information. American and Canadian intelligence services are subject to freedom-of-information legislation. In South Africa the intelligence services have been temporarily exempted from having to produce manuals, part of the provisions of the PAIA. Yet other countries, such as Canada, produce detailed and extensive manuals.

The remit of access to information legislation is often extended by legal challenges by members of the public. However, probably more important in this regard is the political culture in a given society, and the extent to which other mechanisms of oversight are available.

POLICY RECOMMENDATIONS

An intelligence information management policy must relate to real challenges, and 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 is to assess which institutions, individuals, and practices face security risks.

The constitution is the basis for determining what should be protected. The bill of rights is unequivocal about the fundamental rights of all those subject to the constitution. These 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 state information.

These principles were taken into account when drafting the legislation under the new constitutional framework.

Currently, most of the information created and held by the intelligence services is routinely classified as 'confidential', 'secret' or 'top secret'. Moreover, under the MISS, officials outside the intelligence services are allowed to classify information in their possession, and limit its disclosure and distribution. As there is very little oversight of this process, information that may not require protection is beyond ordinary public scrutiny. What is needed is a clear and unambiguous policy framework for security classification by all public bodies, effectively codified in the law. In formulating such a framework, policy-makers need to determine whether information is currently being classified as a matter of habit and convention, or because it really places the state at risk in any way. This area needs further research, which needs to be commissioned and managed.

Security classification amounts to little more than placing a stamp on a document. It is meant to deter officials from disclosing the information in question. Protection should be readily afforded to information whose disclosure could present serious risks to the lives of agents and informants, in pursuit of a legitimate function derived from the mandate of the intelligence services. And the necessary penalties should also be readily imposed on those who violate the requirements of confidentiality.

Technological developments need to be taken into account when assessing the value of the intelligence services' classification of records at different levels of secrecy. Technology has developed to such a point that most governments admit that all information is vulnerable to unauthorised access and disclosure. Consequently, governments are spending very large sums of money on securing their information systems. The myriad of satellite, digital, and electronic transgressions that are now possible means that governments may not even realise that they are losing highly sensitive information to other parties. Therefore, any comprehensive strategy for classifying and declassifying information needs to take technological advances into account.

Another key issue is whether South Africa really needs the Protection of Information Act. The aim of the Act is 'to provide for the protection from disclosure of certain information'. Apart from listing the many parties unauthorised for disclosure, the Act spells out the scope of such information. By definition, this includes 'prohibited places', such as defence installations 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.

Some analysts regard the act as something of an anomaly, given that it co-exists with legislation that guarantees public access to information held by the state. They claim it not only conflicts with the spirit of PAIA, but is all the more odious because it originates from the apartheid days. 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, movement of persons, or institution declared as a hostile organisation through a promulgation of the president.

Despite these sentiments, there is perhaps a more realistic approach. Most would agree that every state needs a legal framework providing for and regulating a degree of necessary secrecy. Laws regulating official secrecy exist in many democracies. PAIA does not protect information, or impose penalties on those who fail to protect it, and the MISS has been criticised for not having any statutory force. Therefore, without anticipating the outcome of a public debate on what state information needs to be protected, a number of principles can be considered to resolve the question of whether legislation should exist 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 full range of policy actors on whom the debate will impact, including non-government organisations, oversight bodies, and the executive.

Next, in keeping with the spirit of the constitution, the framework for the debate should be the constitutional principles of access to information, and the reasonable limitation of this right. And, given South Africa's history, the protection of statutory information should prohibit the state from abusing, manipulating, and destroying information for its own ends. In other words, in terms of this new paradigm, not only individuals and organisations but also the state could be deemed guilty of violating their duty to protect the information for which they are responsible.

Lastly, espionage should be clearly defined as a separate offence, one committed by states with intentions hostile to South Africa's interests. However, the actual content of the crime of espionage should be reconsidered within the paradigm of sharing information.

PRINCIPLES FOR MANAGING INTELLIGENCE INFORMATION

The security forces, particularly the intelligence community, currently classify virtually all information they produce as either Top Secret, Secret, Confidential, or Restricted. If the security services were to adopt a more proactive approach to declassifying information, there would be less antagonism between a public seeking access to information and those who consider the information too secret to share, believing that they are acting in the interests of national security.

A well-regulated classification and declassification system would have two purposes. The first would be to have a uniform system for evaluating, categorising, and safeguarding official information whose unauthorised disclosure could threaten the country's security. The second would be to routinely review the original criteria for withholding information from the public with the intention of making such information publicly available once its disclosure poses no further threat to the country's security.

PAIA's exemptions in fact provide for government secrecy. However, there are costs to this secrecy, including that of physically protecting secrets, the danger of losing public confidence through non-disclosure, and the input and debate limitations. Furthermore, secrets are vulnerable to leaks which can have untold consequences. So the implementation and usage of these sorts of provisions should not be taken lightly.

Several concepts can probably be incorporated into a classification and declassification policy framework. The 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 which procedures. Any new legal framework for classification and declassification should be aligned to PAIA. As PAIA is concerned with disclosing rather than protecting information, grounds exist for additional legislation to protect and classify information. The authority to classify information should be linked to the degree of classification required. For example, only designated office-bearers such as the president, ministers, and heads of department should be entitled to classify information as 'top secret'; lower level officials should only have such authority if it is specifically delegated to them.

Legislation for the classification and declassification of records should incorporate the concept of a life-cycle of secrets, because over time the sensitivity of information and the resources needed for its physical protection may diminish. Moreover, classification should not be used to conceal violations of the law, inefficiency, or administrative error; prevent the embarrassment of a person, organisation or agency; withhold basic scientific research information not clearly related to national security; or conceal previously declassified information.

Lastly, uniform national standards for declassification should be formulated, and their implementation monitored by an appropriate oversight body.

TOWARDS A POLICY FRAMEWORK FOR MANAGING THE RECORDS OF THE INTELLIGENCE SERVICES

What has emerged from this study is that a policy framework is needed for the protection of certain kinds of formation, while ensuring that information about the security services is routinely provided to ensure greater transparency and accountability, and promote informed debate about their performance and role. It should contain appropriate standards for classifying and declassifying intelligence records. The main categories, and the arguments that should be considered in formulating them, are discussed below.

RECORDS CONCERNING THE DAY-TO-DAY OPERATIONS AND MANDATES OF THE INTELLIGENCE SERVICES

The records of the intelligence services are public records, and as such are subject to PAIA. As PAIA expresses a constitutional prescription, the exclusion of the intelligence services from the Act or any of its provisions should not be encouraged.

Instead, the services should begin by considering why their records need to be protected, starting with records about their day-to-day functioning. The intelligence services author and gather significant records in the course of gathering domestic and foreign intelligence, and fulfilling their counter-intelligence responsibilities. The director-general of SASS, Hilton Dennis, suggests that a useful distinction can be made between corporate information and intelligence information (interview, 25.07.2005).

Corporate information would include information about the administration of the services, including their legal mandate and mission, human resources management, policies and procedures, finance, assets, and transactions with corporate and services structures. Regulations issued by the minister and directives issued by the director-general could also be included. The services would have to motivate why any of this information requires protection, and demonstrate how releasing it would harm the country. As far as possible, the grounds for keeping records secret should be aligned to those contained in PAIA.

In order to avoid inconsistencies when dealing with requests for information, the intelligence services should consider institutionalising public annual reports, which would include minimum corporate information. At the same time,

the intelligence services should seek legal opinion on whether the information they wish to protect can be accommodated within the provisions of the PAIA. PAIA also requires voluntary disclosure, and the services would comply with this by releasing information in their public annual reports. Such reports would contribute to a broader understanding of how the intelligence services function, and help to demystify a subject little understood by most people. The challenge in a country such as South Africa is to reach the mass of people, which, given high poverty and illiteracy levels, would require creative grass-roots strategies such as using the radio and visiting local communities.

The second category of information is intelligence information, which can be broken down further into operational information and intelligence reports. The Intelligence Services Act requires the directors-general of the intelligence services and the head of SANAI to take all necessary steps to protect the identities of members of the services, the methods of intelligence gathering, and intelligence sources. Therefore, releasing all known or available categories of information could obviously be risky.

If the intelligence services feel strongly that certain categories of information need to be protected, one option would be to lobby for amendments to PAIA so that categories contained in the Intelligence Services Act, such as methods of intelligence collection, the identities of informers, and other operational details could be incorporated as grounds for refusal. However, the intelligence services would have to accept the right of other interested parties, including freedom of information advocacy groups, to argue for or against any legislative changes.

It has been suggested that South Africa should have a law that explicitly criminalises espionage (interview with Hilton Dennis, 25.07.05). While this was partly the intention of the Protection of Information Act, its provisions are extremely broad, place onerous restrictions on members of the civil service and society, and criminalise the release of vast categories of records, even when no harm was intended or has resulted. Many governments the world over are moving towards greater sharing of information. A South African espionage law would have to consider carefully what state information would be considered harmful to the country's interests if disclosed to or accessed by a foreign government, and how such activity would be framed in criminal law. It would have to take into account the laws that are the basis of co-operation between many countries and already deal with specific crimes such as foreign military assistance, money laundering, and corruption.

The more open and accountable governments are to their own people, the less they have to hide from other governments. As there is no citizenship restriction on

who can access information via PAIA, determined governments wanting to access certain information can easily do so. However, PAIA already exempts certain categories of information, including cabinet records, and records of members of parliament and provincial legislatures. Therefore, if agents of a foreign government access those records, this would well constitute a crime of espionage.

CLASSIFIED RECORDS CONCERNING THE RELATIONSHIP BETWEEN THE SERVICES AND THEIR MEMBERS

One of PAIA's aims is to give individuals the opportunity to access state records about themselves, in order to correct those records. Like all employers, security services are required to keep personal records about individuals, and normally should not have any reason to withhold such information from an individual.

Problems arise when an employee who is in dispute with the service seeks information to use in an internal procedure or in litigation. Albeit in a different context, the Southwood judgment (TPO 161) underlined the need for public bodies to follow fair and proper administrative procedures, and found that classifying a record as confidential does not constitute grounds for withholding it. The service concerned would have to demonstrate that the document has been considered with severance in mind, even if it contains third party information such as a colleague's testimony about the member. The presumption is in favour of disclosure, and everything should be done to make it possible to release the document in question.

The most challenging subcategory in this scenario relates to security clearance investigations. The National Strategic Intelligence Act of 1994 requires the directors-general of the security services to provide security screening procedures for individuals who handle classified information. Records generated in the course of a security screening could be regarded as operational, as their disclosure could harm the procedure. However, the court would probably consider the timing of the request, the administrative fairness of the screening procedure, and whether severing parts of the record had been considered. In such a situation, with South Africa's strong rights-based culture, the courts are likely to consider other rights, including the right to work and the right to dignity.

At the same time, the right to privacy contained in the constitution, and the impending introduction of privacy legislation, is likely to have an impact on how the intelligence services respond to requests for access to their files by the subjects of security clearances. This should encourage greater professionalism, care, and objectivity in handling the vetting process.

CLASSIFIED APARTHEID-ERA RECORDS

Another scenario requiring policy is requests for access to apartheid-era records, such as the TRC files. Apartheid-era state records are likely to remain an area of interest and contestation. Several submissions to the CDRC established by Minister Sisulu suggested that these records should be urgently audited and placed in the custody of the National Archivist. The main concern is preserving the integrity of the records, especially in light of the massive destruction of records during the final years of apartheid. The proposed audit would consider reasons for keeping the records out of the public eye. The process would require considerable resources and should include not only members of the security and intelligence services, but also other social stakeholders such as parliament, non-government organisations, and the judiciary. The IRC process, which was confined to members of the security establishment, was deficient in two respects: quality, probably because of the team's limited experience; and the credibility of its findings, which were not made public.

There is merit in putting the ghosts of apartheid to rest. Considerable public unease is created by claims of alleged apartheid government spies that surface from time to time. An agreed 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 comfort those who believe that the truth has been suppressed. This is not to suggest that the TRC be reopened, but that a responsible way is found to release the information into the public domain. The examples of the former East European states in managing access to the records of former security services provide useful and varied lessons in how to approach this sensitive issue.

At present, PAIA is used by applicants wanting to peruse apartheid files, most commonly about themselves. The state official (in this case the National Archivist) who considers such requests is in a powerful position, and must decide whether or not the file in question contains information that must be severed. Yet these records relate only to individuals and not to the policy decisions and directions from political leaders, who were the architects of the system. Government should look at a mass declassification of all such remaining records, and provide the resources to ensure a credible process.

CLASSIFIED RECORDS ABOUT THE TRANSITION

The transition to democracy marked a significant point in South Africa's political history. There can be little justification for withholding information about this period from the public, including records of the subcouncil on intelligence and its subcommittees established under the TEC. These structures were involved in defining the principles and ground rules for intelligence services operations and, at the same time, trying to steer the existing services towards amalgamation under a future, democratically elected government. The South African transition is held up as a model for the transformation of intelligence services. It is not clear where these records are being kept and whether their integrity has been retained, despite their enduring archival and historical value. The bulk declassification and release of documents from that period would definitely result in a deeper understanding of that process. Determining whether any documentation should not be released would be done by applying the PAIA criteria; but, by and large, those records should be declassified. The intelligence services should use and encourage historians to write the history of their establishment, using this repository of records.

RECORDS OF OVERSIGHT AUTHORITIES INVESTIGATING THE INTELLIGENCE SERVICES

A number of oversight institutions can at any one time be required to investigate a matter concerning the intelligence services, and consequently access classified information. These include the Inspector-General for intelligence, the JSCI, the Human Rights Commission, and the Public Protector.

When deciding on the most appropriate and effective investigating structure, a dual approach should be considered which would link an instrument with access to intelligence information to a public investigative process. This recommendation emerged from the work of the Hefer Commission commissioned by Sisulu (Levy 2004). For example, a commission of inquiry or the Human Rights Commission could involve the Inspector-General for intelligence, who has full access to the intelligence services (which they do not). This would also inspire public confidence in the outcome of the inquiry.

THE STORAGE OF INTELLIGENCE RECORDS

The records of the intelligence services are public records, and therefore have to be managed in terms of the National Archives Act. In 1999 the NIA entered into an agreement with the National Archives relating to the implementation of the

Act. Among other things, the parties agreed on previously unclear aspects of the requirement that records be transferred to the custody of the National Archives for preservation and custodianship. Given that the NIA's records required special management, the parties agreed that the NIA could retain the records on its premises, but in strict accordance with archival standards of safekeeping and classification. The National Archives would train NIA staff. As a result, the NIA is in compliance with the National Archives Act, and its filing of records has improved over the years (interview with Peter Richer, 09.09.2008).

Two factors have accelerated the drive towards better and more efficient management of records. The first is the need to comply with PAIA; the NIA now needs an orderly house if it is to respond to requests for information in a timely manner. The other has been the need to protect its information. A series of detrimental leaks has pointed to the vulnerability of the organisation, and prompted management to introduce measures and systems that streamlined the flow of information and made it easier to monitor who had access to records. The use of an effective document management system has also made it easier to monitor who authorises decisions. These systems are both of archival value, and improve information security. In addition, over the past decade the NIA and SASS have introduced disaster recovery plans to avert the permanent loss of data. These developments are very positive, and any policy head should ensure that such standards of information management are adhered to by the entire intelligence community. Without proper records management, there can be no meaningful access to information.

CONCLUDING REMARKS

What should be secret, and why? What should the public know, and why? Under what conditions should it be a crime to hide, destroy, or distort information, and what should be the penalties? What should the penalty be for releasing information without authority? Who should classify and declassify information? What is 'Top Secret' in today's world? And when does a secret expire? These are some of the questions that have prompted this study and which hopefully have been at least partially answered.

But who will guard the guardians? The post-apartheid intelligence services have not uniformly resisted the promotion of access to information. In some instances, without having to be pushed, they have taken laudable initiatives to make themselves known to the public.

Together with the HRC, parliament has a special duty to ensure that the intelligence services are as transparent and accountable as possible. In fact, it is

ultimately the duty of parliament to consider the legal framework for transparency. Over and above this, the institutions who are meant to oversee and investigate the intelligence services where required – the Inspector-General and Auditor-General – must do so vigorously. But there is a worrying factor that may limit parliament in playing this role in a robust way. Except for the HRC, the structures with oversight of the intelligence community all operate within the intelligence services' circle of secrecy, and accept whatever the intelligence services considers as classified. These oversight authorities need to start questioning why certain information has been designated secret, at least in the formative stages of defining (or redefining) a transparency and secrecy policy.

Strong leadership and policy direction will be needed. Some members of the intelligence services may feel threatened by a paradigm that does not regard them as being the determining force behind a policy review, but rather as servants of its outcome. Such a reaction would be understandable; the intelligence services have long been in the paternalistic position of deciding who should know what. However, parliament should ensure that the services clearly understand the broader issues involved, including the historical and constitutional imperatives; create appropriate policy frameworks for the services; and review their mandates.

Parliament must take stock of the failings of PAIA as well as other relevant legislation. Lastly, the minister of intelligence services must ensure that adequate resources are available to make voluntary disclosure a reality, and parliament must keep watch over how this duty is performed.

INTERVIEWS AND REFERENCES

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 when interviews were conducted.*

REFERENCES

Legislation

South Africa

Republic of South Africa. 1978. Bureau for State Security Act, No. 104, 1978.

Republic of South Africa. 1972. Security Intelligence and State Security Council Act, No. 64, 1972.

Republic of South Africa. 1982. Protection of Information Act, No. 84, 1982.

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.

Republic of South Africa. 1994. National Strategic Intelligence Act, No. 39 of 1994.

Republic of South Africa. 1994. Intelligence Services Control Act, No. 40, 1994.

Republic of South Africa. 1995. Promotion of National Unity and Reconciliation Act, No. 34, 1995.

Republic of South Africa. 1996. National Archives Act, No. 43, 1996.

Republic of South Africa. 1996. The Constitution of the Republic of South Africa, No. 108, 1996.

Republic of South Africa. 1999. Public Finance Management Act, 1999.

Republic of South Africa. 2000. Promotion of Access to Information Act, No. 2, 2000.

Republic of South Africa. 2002. Intelligence Services Act, 2002.

Republic of South Africa. 2002. Electronic Communications and Transactions Act, No. 25 of 2002.

Republic of South Africa. 2002. Regulation of Interception of Communications and Provision of Communications Related Information Act, No. 70 of 2000.

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.* Pretoria.

Task Group on Open Democracy. *Open Democracy Act for South Africa. Policy Proposals*. 19 January 1995.

RSA Parliament. Annual Report of the Joint Standing Committee on Intelligence, 1997.

RSA. Report of the Auditor-General on the audited financial statements of the intelligence services, 1996/1997. Pretoria.

RSA. Report of the Auditor-General on the audited financial statements of the intelligence services, 1997/1998. Pretoria.

South Africa. Hansard, 12 May 1996.

United States

United States of America. 1997. *Report of the Commission on Protecting and Reducing Government Secrecy (Moynihan Commission Report)*. 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).

Other

United Nations. 1994. *United Nations Development Report.*

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

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.

AlMashat, 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). 1992. *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. (eds) 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 peacekeeping, 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. (eds) 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.

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 counterrevolutionary 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 (pp. 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.

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.

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.

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.

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 F.W. 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, (pp. 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.

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, R. 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 Professional Privelege, in Oosthuizen, G.C., Shapiro, H.A. & Strauss, S.A. Professional Secrecy in SA. A symposium. Cape Town: Oxford University Press.

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. Decisionmaking 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: Sedgwick.

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.

WELL-KEPT SECRETS

South Africa's democratic constitution entrenches citizens' right of access to information held by the state. In this volume, the author – who previously held a senior position in the intelligence community – assesses whether the post-apartheid intelligence services have complied with this obligation during the first decade following South Africa's transition to democracy.

She raises key normative questions such as whether relevant policy-makers and the intelligence services have pursued appropriate and meaningful levels of transparency; and whether there has been a decisive break with the culture of secrecy that characterised the apartheid intelligence apparatus. Drawing on international theory and comparative experience, she spells out a path towards clearer policy and practice on these vital issues.

It is hoped this book will help role players in the intelligence dispensation to gain greater clarity about the boundaries between transparency and secrecy – and, equally crucially, equip citizens to better defend their hard-won constitutional freedoms.

INSTITUTE FOR

GLOBAL DIALOGUE

FRIEDRICH EBERT STIFTUNG

ISBN 978-1-920216-22-1