The Promotion of Access to and Protection of National Security Information in South Africa

Jonathan Klaaren
Professor, School of Law, Co-Director of the Research Unit on Law and Administration, University of the Witwatersrand
Visiting Scholar, Center for the Study of Law and Society, University of California (Berkeley)
klaarenje@law.wits.ac.za

5 May 2003, Washington DC

Introduction: The Promotion and the Protection of Information[1]

The two South African statutes most relevant to national security information have similar titles but essentially approach the issue from opposite perspectives. The Promotion of Access to Information Act and the Protection of Information Act also come from two different eras in South Africa national history.

South Africa's constitutional right of access to information is implemented through the Promotion of Access to Information Act 2 of 2000 (AIA). This legislation gives effect to and is itself mandated by the post-apartheid Constitution, generally acknowledged as global progressive. In one of the legislation's innovations, the AIA extends the ambit of right to information to the private sector. The AIA was enacted in 2000 and has fully taken effect, although some of its compliance deadlines have been extended.[2]

The national security ground of refusal to access to information is contained in section 41 of the AIA.[3] That section protects information the disclosure of which could reasonably be expected to cause prejudice to defence, security, or international relations. It also protects information required to be held in confidence due to an international agreement or supplied by another state in confidence. The ground is discretionary and may be waived. In the South African transition, an early and

[1] The first several sections of this chapter draw on J Klaaren 'National Information Insecurity? Constitutional Issues Regarding Protection and Disclosure of Information by Public Officials' in (2002) 119 South African Law Journal 721-732.

[2] See generally, I Currie and J Klaaren The Promotion of Access to Information Act Commentary (SiberInk, 2002). Current developments regarding the AIA are available at the RULA website at www.law.wits.ac.za/rula.

[3] See I Currie and J Klaaren The Promotion of Access to Information Act Commentary (SiberInk, 2002) 173-177 for a more detailed examination of section 41.

significant judicial commission of enquiry established the principle that foreign policy embarrassment is an insufficient reason for non-disclosure of military information.[4]

This paper will not focus either on the AIA generally or on the outlines of section 41 specifically. Instead, the most significant feature of the AIA with respect to national security information in South Africa is not what the AIA does but rather what the AIA does not do. The AIA does not repeal pre-existing government secrecy and confidentiality laws. Even after the enactment of the AIA, the disclosure of the information through any means other than in response to a formal access to information request remains subject to law and regulations preserving confidentiality in government. These laws and regulations include the Protection of Information Act of 1982. The AIA does not strike down those laws and regulations. This is the case even though the AIA does apply to their exclusion in respect of formal AIA requests for records.[5] These laws and regulations restricting the disclosure of information by current and former public officials of course remain subject to the constitutional rights of access to information and freedom of expression.

The current centrepiece of South African legislation restricting disclosure of information is the Protection of Information Act 84 of 1982. This Act replaced the Official Secrets Act 16 of 1956. The Protection of Information Act is very broad in its pursuit of government secrecy. A look at the wording of section 4 of the Protection of Information Act illustrates its breadth. Subsection 4(1)(b) targets 'any person who has in his possession or under his control or at his disposal ... any document, model, article or information ... which has been entrusted in confidence to him by any person holding office under the Government ... or which he has obtained or to which he has had access to by virtue of his position as a person who holds *or has held office* [or a contract] under the Government ... and the secrecy of which ... he knows or reasonably should know to be required by the security *or other interests* of the Republic' [emphasis added].[6] This subsection prohibits the disclosing of the information to a non-authorized person as well as failing to take care of such information. The following subsection prohibits the receiving of such a document. Section 4 thus makes little or no distinction between information that should not be disclosed because of its military or national security significance and other information held by the public service that should not be disclosed. Further, section 4 makes no distinction in its application to current and former public officials. The extent of application of section 4 has real consequences: a violation of section 4(1) is made an offence punishable by up to 10 years imprisonment and a fine.

---

[4] The Cameron Commission determined that South African policies regarding the provision of weapons to countries with poor human rights records should be made public. J Klaaren and G Penfold 'Access to Information' in M Chaskalson et al. (eds) Constitutional Law of South Africa (Juta, 2002) 62-21.

[5] In an important difference from the US Freedom of Information Act, the AIA does not reference or incorporate a classification system for the information security of records. Civil society resisted attempts to use the language of classification during the drafting of the legislation.

[6] The text quoted here is taken from s 4(1)(b)(iii) and (iv). Section 4(1)(b)(v) is even broader.

Other sections of the Protection of Information Act appear to be more narrowly intended for national security or military use.[7] For instance, section 3 contains a prohibition in 3(a) on the obtaining of information 'used, kept, made or obtained' in any prohibited 'place', which is primarily defined to include defence works and armaments production facilities. Section 3(b) also prohibits the preparation or compilation of a document relating to the 'defence of the Republic, any military matter, any security matter or the prevention or combating of terrorism'. Both of these actions are criminalized and there is a purposive requirement to both.

Without engaging in a detailed or comprehensive examination of section 3 of the Protection of Information Act and section 41 of the Promotion of Access to Information Act, it is clear that the AIA takes a detailed and particularized approach to the determination of legitimate disclosure of military information. This can be contrasted to the more categorical approach of the Protection of Information Act. While the AIA does include a categorical sub-section, it also gives examples of what will fit within that category. On the whole, the AIA approach is less susceptible to expansion.

Implementation of the Protection of Information Act: The Minimum Information Security Standards (MISS)

Of course, it is not enough to look at the law on the books. One must examine the law as it is implemented. The principal mechanism by which the Protection of Information Act is currently implemented is a Cabinet-level policy document. This is the document on Minimum Information Security Standards (MISS). The Minimum Information Security Standards document was approved by Cabinet on 4 December 1996 as 'national information security policy' and has not been updated. As policy, the MISS is to be implemented by each public institution as well as by some private institutions working with public ones. According to its preface, the MISS 'must be maintained by all institutions who handle sensitive/classified material of the Republic'. Each institution is to compile its own rules of procedure using the MISS policy as a set of minimum standards.[8]

Despite the department-level application of the MISS policy, the leading role in the implementation of the MISS is taken by the National Intelligence Agency. The NIA is one of the several security institutions set up by the South African Constitution and legislation. It is subject to special procedures of Parliamentary accountability. NIA security advisers are available to advise public institutions on MISS implementation.[9]

---

[7] Section 5 criminalizes providing aid to gain access to a prohibited place. Further sections of the Protection of Information Act regulate the onus of proof and other incidental matters. Other legislation targets specific sectors such as the Defence Act 44 of 1957 and the Armaments Development and Production Act 57 of 1968.

[8] Para 5, MISS.

[9] Para 8, MISS.

Moreover, the NIA is responsible for issuing amendments to the MISS.[10] As a general policy applicable to all government departments, this aspect of the implementation of the MISS can draw only upon the force of section 4 of the Protection of Information Act.

It is important to realize that a separate specific policy governs information security within the South African Defence Community. This more narrow military information security policy is contained in a set of South African National Defence Force Orders (SANDF/INT DIV/2/97). This policy applies principally to the SANDF and Armscor.[11] Furthermore another set of separate policies govern the South African Police Service and the South African Secret Service.[12] The implementation of information security within the security services could draw upon the force of all sections of the Protection of Information Act and not merely section 4.

What is also crucial to realize is that the information covered by the SANDF Order is much narrower than the information covered by the MISS. Indeed, the SANDF policy would appear to be both narrower in application and more broadly supported in law than the MISS itself. Essentially, the SANDF policy covers only military or traditional national security information. It is not through its application provisions but rather through its content definition that the scope of the SANDF Order is restricted. In other words, it is the kind of information and not the kind of public body that limits the operation and coverage of the SANDF Order. In the SANDF Order, 'classified information' is defined as:

> any information or material which is held by or for, is produced in or for, or is under the control of the State or which concerns the State and which for the sake of national security be exempted from disclosure and must enjoy protection against compromise. Such information is classified either Restricted, Confidential, Secret, or Top Secret according to the degree of damage the State may suffer as a consequence of its unauthorised disclosure.[13]

From the point of view of history and bureaucratic policy development, it seems obvious that the MISS is based upon a military/national security information classification scheme roughly similar to that one presently contained in the SANDF Order.[14] In other words, the MISS is more or less a cut and paste from an earlier

---

[10] The preface notes how the MISS will be amended and such amendments distributed: 'Any comments or recommendations in respect of this policy must please be forwarded in writing to the Chairperson of the Functional Security Committee of NICOC. All amendments to this policy will be issued by the National Intelligence Agency being the department national responsible for counter-intelligence. Government departments, institutions, parastatals and private companies will be responsible for the distribution of such amendments within their own organisations.'

[11] Institution is defined to mean 'any department of State, body or organisation that is subject to the Public Service Act or any other law or any private undertaking that handles information classifiable by virtue of national interest.' SANDFO/INT DIV/R/2/97 A-2.

[12] See Appendix A of the MISS.

[13] SANDF Order A-1.

[14] See for instance, para 3.1 and para. 4.

version of the SANDF order. Presumably, this occurred at some point in the 1980s when the national security state was ascendant and the influence of the South African military was at its peak.[15]

This brings about a significant difference that opens the MISS to constitutional challenge. The meaning of the term 'classified' in the MISS is much broader than the term 'classified' in the SANDF Order. Classified no longer has the substantive meaning of national security. Instead, in the MISS it means:

> Sensitive information which, in the national interest, is held by, is produced in or is under the control of the State or which concerns the State and which must by reasons of its sensitive nature, be exempted from disclosure and must enjoy protection against compromise.[16]

This history contributes to the overbreadth of the MISS. In essence, the MISS definition of classified information has the shell of the military definition but with its heart -- the reference to national security -- cut out. The term 'sensitive' has replaced 'national security'. The result is circular. Instead of a substantive, military-based reason for non-disclosure, we have the general reference to 'sensitive information ... which by reasons of its sensitive nature [must] be exempted from disclosure'. Interpreting the MISS most broadly, a military information security policy has been crudely and inappropriately adapted to attempt to cover the entire public sector. While this can and has been argued to be justified along the lines of how economic espionage has replaced military espionage in the new global economy, it is nonetheless a far cry from the traditional definition of national security.[17]

Dating from what must be a history subsequent to the one just described, the MISS also shows internal evidence of its conflict with the constitutional right of access to information. Together with the preface, the use of the phrase 'must be exempted from disclosure' in the MISS definition of classified information shows that the MISS in its post-apartheid version was revised within the legal context of the right to information. Read in context with the preface of the MISS, it is clear that this phrase derives directly from the policy proposals and from the draft Open Democracy Bill (the precursor to the Promotion of Access to Information Act).[18] Indeed, the MISS itself foregrounds its allegiance to the AIA in the preface: 'Our need for secrecy and therefore information security measures in a democratic and open society with transparency in its government administration according to the policy proposals regarding the intended Open Democracy Act have been taken into account'. This reference to the policy of the Promotion of Access to Information Act becomes even more specific in Chapter 1 of the MISS:

---

[15] For a historical examination of the military and the South African state, see A Seegers The Military and the Making of Modern South Africa (1996).

[16] MISS p. 8.

[17] Of course, one could argue that the South African (e.g. apartheid) tradition was precisely to define national security beyond military/security/intelligence matters.

[18] See MISS Preface and para 4.

> Although exemptions will have to be restricted to the minimum (according to the policy proposals regarding the intended Open Democracy Act), that category of information which will be exempted, will as such need protection. The mere fact that information is exempted from disclosure in terms of the Open Democracy Act, does not provide it with sufficient protection. ... *Where information is exempted from disclosure*, it implies that security measures will apply in full. This document is aimed at exactly that need: providing the necessary procedures and measures to protect such information. *It is clear that security measures do not concern all information* and are therefore not contrary to transparency, but indeed necessary for responsible governance.[19]

One could even argue to a court that these references by the MISS to the AIA mean that properly (and narrowly) interpreted there should be no conflict between the substantive information disclosure policy of the Promotion of Access to Information Act and the substantive information disclosure policy of the MISS. Since the MISS itself claims to be within the spirit of the AIA, the AIA should clearly trump the MISS.[20]

Practices of the MISS: Security Clearance and Institutional Procedures

That benevolent interpretation has not been the one put into practice. As one might expect of an apartheid era information policy, the spirit of the MISS and in particular its security screening procedures run almost directly counter to the spirit and purpose as well as the procedures and institutions of the Promotion of Access to Information Act. In practice, the MISS is a de facto government general confidentiality policy. The remainder of this section describes the information security implementation procedures of the MISS: a security clearance procedure and a procedure for signing declarations as well as monitoring by the NIA.

The main feature of the implementation of the MISS is a security clearance procedure.[21] With respect to governmental and parastatal personnel, the investigation phase of the security clearance process is conducted by the Crime Combating and Investigation Division of the South African Police Service.[22] In order to obtain a security clearance, a public service employee must complete a 9-page Security Clearance Form (Z204).[23] It may be that interviews are conducted in some cases.[24] SAPS will then

---

[19] MISS paras 3 and 4, chapter 1.

[20] In other words, the definition of classified information in the MISS could (and one can argue to a court *should*) be interpreted only to cover information which must -- in terms of some law or policy deriving from or consistent with the AIA -- be exempted from disclosure. See further 'National Information Insecurity?'.

[21] One could make an AIA request for the number of employees in government with security clearances beyond the security services. From conversations with public officials, it appears that the information security measures are inconsistently applied even at senior levels.

[22] See Appendix A of the MISS.

[23] This form is provided in Appendix D of the MISS.

[24] The controversy regarding the questioning of members of the Presidential press corps on sexual partners and relationships indicates the extent to which questioning either by questionnaire or in an interview may go, although those questions were posed by the Secret Service, a separate security/intelligence service from the NIA. See V Harris 'Sex, Spies, and Psychotherapy' available at http://www.wits.ac.za/saha/foi_reports.htm.

recommend security clearance. The actual decision-making is the responsibility of each institution.[25]

While the institutional centrepiece of the MISS is this security clearance procedure, it is clear that monitoring of the procedure by the NIA is a significant feature. As the implementor of the MISS and the agency charged with the defensive aspect of counter-intelligence (e.g. information security), the security clearance process implementing the MISS is coordinated and monitored by the National Intelligence Agency. As such the NIA is tightly linked to the operation and continual monitoring of the security clearance and information security procedures. For instance, in an apparently standard letter granting security clearance, heads of directorates are requested to 'see to it' that the person's behaviour (once granted a security clearance) is irreproachable. Further, 'any breach in security, disembodiment of security measures or risky security behaviour must immediately be report to the Direction: Administration [NIA], so that the situation can be investigated'.

In addition to the security clearance procedure (but possibly linked to that procedure in practice), Appendix B of the MISS contains a standard form for a declaration relating to the Protection of Information Act. The declaration states that the signatory is familiar with the Protection of Information Act and more particularly with section 4. A signatory of a declaration might be presumed to have read the provisions of section 4 which are printed on the back of the form. The declaration goes to state:

> I realise that I am guilty of an offence should I disclose any information I have at my disposal on account of my office and in respect of which I know, or should reasonably know, that the security of other interests of the Republic demands that such information be kept secret, to anyone other than a person lawfully entitled to it; or a person to whom I am in duty bound to disclose it in the interests of the Republic; or a person to whom I have been authorised to disclose such information either by the Head of Department or another officials authorised by him.

Furthermore, the declaration states 'I realise that the above provisions and instructions are not applicable during my term of office only, but also after my services in the Department have been terminated'.

There is no apparent express authority in the Protection of Information Act for these declarations. In at least some departments, the declaration may be required as part of the security clearance process.[26] Technically, the declarations do not add any legal force to the prohibition against disclosure of information contained in the Act itself. Nonetheless, they presumably would aid the State in a prosecution in terms of the Act. The signed declarations would assist in demonstrating that an accused knew or reasonably should have known about the terms of section 4's prohibition on disclosure.

---

[25] See MISS, para 10.1, p. 50.

[26] The only reference to the declaration in the MISS is in responsibilities of heads of institutions where one responsibility is to 'ensure that persons dealing with classified matters sign the prescribed declaration of secrecy (see Appendix B, a draft declaration that can be modified to suit the requirements in each particular case)[.]' MISS, para 10.5, p. 51.

Constitutional Prospects of the Protection of Information Act and the MISS

As I have argued more fully elsewhere, the security clearance, NIA monitoring, and declaration signing procedures of the MISS clearly inhibit and endanger the South African constitutional rights of access to information (s 32) and freedom of expression (s 16).[27] In addition to the direct application of these constitutional rights, the South African Constitutional Court has made it clear that where administrative discretion may impinge upon these rights, Parliament must be careful to provide clear guidelines for the exercise of such administrative discretion.[28] Where no such guidelines are provided by Parliament, the section enabling such administrative discretion is more likely to be found to be unconstitutional.

One important case decided in the Southern African context supports the argument for partial unconstitutionality of the Protection of Information Act.[29] In a case reported in 1996, *Kauesa v Minister of Home Affairs*, the Supreme Court of Namibia invalidated a regulation which made it an offence for a member of the police force to comment 'unfavourably in public upon the administration of the force or any other Government Department'. The unfavourable comment at issue in the case was a comment on affirmative action in the Namibian police force. The court balanced the interest of the citizen member of the police force in expression with that of the state in maintaining discipline, efficiency and obedience in the police force. The regulation was determined to be unconstitutional and not justifiable because it was vague and overbroad and because it was not proportional to its objective.

In particular, the portion of the MISS policy implementing information security beyond the security institutions (e.g. in public institutions beyond NIA, SASS, SAPS, and SANDF) is arguably unconstitutional in its effect. The National Intelligence Agency and other public bodies are likely to run into serious trouble enforcing section 4 of the Protection of Information Act through the MISS. Section 4 is likely to be unconstitutional on its face either as vague and overbroad[30] or as a direct infringement of the constitutional right of freedom of expression (perhaps read with access to information) or as a combination of its breadth and its restriction on fundamental rights.[31] Unless the scope of the MISS is restrictively interpreted in line with the AIA, the same unconstitutional fate awaits its provisions. In any case, the finding of unconstitutionality

---

[27] See 'National Information Insecurity?'.

[28] See Dawood v Minister of Home Affairs 2000 (3) SA 936 (CC) (state may not depend upon the limitation clause where a fundamental right is implicated and no guidelines are provided).

[29] 1996 (4) SA 965 (NmS). This discussion is taken from Marcus and Spitz, below.

[30] Thereby violating either the principle of legality or the right to just administrative action or both. Still, the charge of overbreadth does not automatically lead to unconsitutionality. Poswa v MEC for Economic Affairs Environment and Tourism, Eastern Cape 2001 (3) SA 582 (SCA) (in anti-corruption context).

[31] The evaluation of unconstitutionality is supported by G Marcus and D Spitz in 'Expression' ch 20 in M Chaskalson et al. (eds) Constitutional Law of South Africa (revision service 3, 1998) at 20-28.

must apply with even greater force to the system of security clearances, NIA monitoring and Appendix B declarations of the information security policy that the Minimum Information Security Standards document sets out to be national policy. To the extent that they are applied beyond the realm of the security services as identified in Chapter 11 of the Constitution, these mechanisms are likely to be overbroad and to illegitimately restrict at least the right of freedom of expression.

Recent Access Events

Two recent events demonstrate the possibilities and tensions for access to information within this framework.[32] The lengthy delay preceding the recent release of the TRC sensitive records demonstrates the continuing power of the intelligence community. Additionally, an analysis of the recent court decision in the C2I2 case also points to the contested understanding of national security information disclosure.

The Sensitive TRC Files.[33]

A long saga has surrounded 34 boxes of "sensitive" TRC records removed from the TRC offices in 1999 and placed in the custody of the Department of Justice (DOJ). These records were the ones judged (although the criteria and authority are unclear) most sensitive of those collected by the Truth and Reconciliation Commission. Using the AIA, a South African non-governmental organization, the South African History Archive (SAHA) secured a list of the files in those 34 boxes. The files include a list of informers and a confidential submission by the ANC. The concern of some professional archivists, including SAHA, was for the safekeeping of these records and for the potential undue influence over and access to those records that might be exercised by the intelligence community.

This concern appears to have been well-founded since the actual custody of the Department of Justice of these 34 boxes over the past few years has never been clear. In May 2001 SAHA put in an AIA access request to the Department of Justice in relation to these records. In December 2001, DOJ indicated that they did not have the records and suggested that SAHA approach the National Archives. SAHA immediately requested clarification in writing from both the National Archives and the National Intelligence Agency (NIA). National Archives did not respond. In contrast, NIA indicated in writing that the records, to their knowledge, were still in the safe custody of DOJ.

During the second week of April 2002, John Perlman of the radio station SAFM ("the station for the well-informed") conducted a series of interviews with key roleplayers

---

[32] Other ongoing conflicts over access to information are also directly relevant to the issue of national security. In particular, the South African History Archive (SAHA) hosted a 2002 conference aimed at exploring ongoing South African government secrecy with respect to the history of South Africa's nuclear weapons and development program. See http://www.wits.ac.za/saha/nuclearhistory/index.htm. Furthermore, SAHA has successfully applied for access to the so-called "sensitive documents", the 8/2 files used by the National Archives for sensitive materials during the 1960s and the 1970s. See http://www.wits.ac.za/saha.

[33] This section draws on V Harris 'Telling Truths About the TRC Archive' available at http://www.wits.ac.za/saha/foi_reports.htm.

in relation to these "sensitive" TRC records. On 9 April the spokesperson for DOJ informed him that the records were with NIA for safekeeping. And on 12 April the NIA spokesperson stated that the records were indeed with NIA, but emphasized that they would be returned to DOJ shortly.

The CCII case and the Arms Deal.

In the late 1990s, South Africa made a large purchase of arms from overseas. This complex set of agreements has been known as the arms deal. The arms deal has generated a number of allegations of corruption and mismanagement. The South African government has investigated some of these instances but has largely continued to claim that the arms deal was largely free of improprieties. Assisted by the Open Democracy Advice Centre (ODAC), a disappointed tenderer, Richard Young, has used the AIA to attempt to access information relating to the decision not to award his company, CCII, with a contract as well information relating to the government investigation of the arms deal. The agency of government primarily involved has been the Auditor-General rather than the Minister of Defence. The request for access to information eventually landed in court and resulted in the first significant judicial decision on the AIA.[34] The result was essentially a victory for requesters.[35] The government was ordered to provide a list of documents available and to justify the documents that were not available. The government initially appealed the court's decision to a higher court. However, in March 2003, the Auditor-General withdrew his appeal of the decision and agreed to apply the provisions of the AIA and to hand over the documents that were not protected from disclosure.

Where To From Here (South Africa)?

The above has described the current articulation and implementation of information security policy by the post-apartheid South African state and explored some of their constitutional and legal weaknesses. It is arguably in the interests of the state as well as of civil society to address these weaknesses and place South African information security policy more clearly on a constitutional foundation. The good government rationale of transparency should be given effect.[36] Furthermore, the broad confidentiality fostered by the Protection of Information Act and the MISS runs directly counter to the latest thinking of the last ten years or so regarding the effectiveness of a public sector in partnership with the private sector. The levels of confidentiality the NIA attempts to impose appear cumbersome and counterproductive.

---

[34] While the CCII case is one that implements the AIA, earlier South African cases had implemented the constitutional right of access to information directly. This is a contrast from the situation in Bulgaria. See A Kashumov 'National Security and the Right to Information in Bulgaria' at 4.

[35] For more background and a legal analysis of this case, see 'Analysis of the Judgment in CCII Systems (Pty) Ltd v Fakie NO (January 2003) available at http://www.wits.ac.za/saha/foi_reports.htm.

[36] See in the 1996 Constitution, the principle expressed to guide the public administration in section 195(1)(g): "Transparency must be fostered by providing the public with timely, accessible, and accurate information."

Research in several areas would provide useful information regarding practical ways forward. Without being comprehensive, several may be mentioned here. First, with respect to the Appendix B declarations, one should attempt to get an indication of their use and effectiveness. Even though these declarations are governing policy, individuals may well refuse to sign these declarations on the above grounds of lack of authority and unconstitutionality. Second, with respect to the security clearance process and the NIA monitoring, one should monitor the extent to which the system is operative in government practice. One should also monitor the existence and operation of general policies of confidentiality in line with the AIA and specifically derivative of the AIA (as well as the imminent Privacy Act) rather than of the Protection of Information Act. It is possible that government policies of information security will be built on a department by department basis with a foundation of AIA principles. This would represent a decentralized approach rather than the older centralized policy.

Based on the research thus far, my view is that the Minimum Information Security Standards cabinet policy should be scraped. The replacement policy should be based upon the provisions of section 41 of the Promotion of Access to Information Act not on the Protection of Information Act. Likewise, the Protection of Information Act itself should be revised to fit within constitutional restraints while still providing for document handling procedures and the classification of national security information.

There are some indications that revision of the MISS and of the Protection of Information Act may soon become priorities of the government.[37] The Minister of Intelligence Lindiwe Sisulu announced in Parliament in June 2002 that a review of the classification of documents should be instituted.[38] In March 2003, she announced the formation of a classification and declassification review committee. This committee has relatively strong civil society representation in its personnel. Further, it is apparently mandated not only to review the criteria and classification of apartheid-era information, but also to review the formulation of the MISS and the Protection of Information Act as well as the National Archives Act and the National Strategic Intelligence Act. It appeared also possible that amendments might be suggested to the Promotion of Access to Information Act. The announced intention was to review the MISS and elevate its status to that of regulations. This would be a significant step towards transparency and would afford civil society significant opportunities to influence the formulation of the revised MISS. This committee has asked for submissions by 30 April 2003 to guide its work.

Three Global Stories

To expand the focus beyond the narrowly national, it may be that South Africa's recent history of information security is at the confluence of three global stories of

[37] This paragraph draws from stories in the Sunday Independent (8 March 2003), the Sunday Times (8 March 2003), and SABC Online (8 March 2003).

[38] Business Day (6 June 2002) 'Apartheid era documents might soon be declassified.'

institutional development.[39] These three stories or trajectories undoubtedly overlap and interact in a variety of ways in different locales and political situations.

The first two of these stories can be traced back to origins in the US. One story is that of the diffusion of national rights to information laws. There has been a rapid diffusion of these laws since the late 1980s. The second story concerns the diffusion of secrecy laws, as Roberts shows in his paper.[40] Based on the model of American military secrecy, there were two bursts of diffusion of these laws, first in the development of NATO and second in the expansion of NATO into the countries of Eastern Europe following the end of the Cold War.

The third story of informational policy development is one that more global and may indeed be one where the South African story itself has played no small role. It is the story that Robert Horowitz tells in his analysis of the developments in the South African communications sector since 1994.[41] In Horowitz's account (although the right to information does not figure prominently), civil society largely won and restructured the communications sector along a model of participatory citizenship. This third story of participatory and informed citizenship seems also to be the story that Deidre Curtin tells in her paper, albeit in the context of information communication technology in the European Union.[42]

It may be that this third story is one that is presently unfolding in Africa and with particular impact. Throughout Africa, ministries of information are facing serious challenges. National information security policies in countries such as Ethiopia and Nigeria are potentially in transition with ongoing legislative drafting efforts for right to information laws. The challenges to top-down government communications strategies come from other government organizations as well as from individuals and new communications technologies and media interests. The reception and impact of mobile phone networks may be one part of this broad trend. This trend may represent more than the adoption of specific laws and may be an expression of an emergent model of participatory and informed citizenship.

The Information-Secrecy Linkage

[39] Here, I am using the notion of stories of development that Alasdair Roberts has employed in a recent paper. See Workshop on the Internationalization of Regulatory Reforms, University of California (Berkeley), 25-26 April 2003. However, my specification of the three stories differs slightly. As explained in the text, for the third story, I see a more global and expanded story of citizenship development within the communications sector rather than a particular move towards greater informational accountability on the part of international financial institutions.

[40] A Roberts 'NATO's Security of Information Policy and the Right to Information'.

[41] Robert B Horowitz Communication and Democratic Reform in South Africa (Oxford University Press, 2001).

[42] D Curtin 'Digital Government in the European Union: Freedom of Information Trumped by "Internal Security"' (see particularly at 13-14).

It may be worthwhile to briefly note that these first two stories described above have some close linkages in practice and in law. The linkage mechanisms between the right to know laws and the secrecy laws may be as important to analyze as their respective substantive policies on national security information. In particular, through several legal mechanisms, these secrecy laws are often incorporated into the content of freedom of information laws. One mechanism is the classification of information by the military. This is the US model. A second mechanism of incorporation is through the explicit presumption granted to another piece of legislation, a secrets law, whose content then in practice trumps that of the right to information law. This may be explicit in the law or through the operation of the later in time rule. This is the situation in Bulgaria and in other Eastern European states.[43] A third mechanism is through the protection of information rendered confidential through international agreements. The content of the international agreement is then imported into the domestic legal order. Even without these legal mechanisms, these secrecy laws may well be enforced through the bureaucratic power of the military. It may be that there are other legal mechanisms as well to link the substantive content of the secrecy rules to the right to information laws.

In South Africa, it is the third of the formal mechanisms that may potentially be used. Section 41(1)(b) of the AIA protects information that is required to be held in confidence by an international agreement. There is an international agreement in force with the United States: the 1998 General Security of Military Information Agreement.[44] However, the operation of this mechanism in the South African context remains untested. Greater research needs to be done on the content and status of the international security agreements that the South African state has concluded with other states.

To date, the Protection of Information Act and the MISS itself have been the sources of the implementation or bureaucratic power exercised by the South Africa military and intelligence communities. The existence of this nationally-driven is an important feature that may distinguish the South Africa national security information policy dynamics from the countries of NATO implementing the Security of Information (SOI) policy of NATO, as Roberts shows. One may use the analysis of breadth, depth, centralization, controlled distribution and personnel controls to analyze the MISS. In these terms, the MISS is one of breadth, centralization, controlled distribution, and personnel controls. The element of depth is however apparently a contested one as the operation of the review classification committee demonstrates.

Within this policy field, the focused interpretive and implementation power of the military/intelligence community certainly overshadows that of the set of government

---

[43] See A Kashumov 'National Security and the Right to Information in Bulgaria'.

[44] Communication from A Roberts (28 April 2003). Obtaining this 1998 Agreement, one could then compare the South African agreement to the breadth, depth, centralization, controlled distribution, and personnel controls of the apparent shape of the NATO policies as well as examine the effect or lack thereof of the agreement on South African informational security law, policy, and practice.

agencies given various responsibilities in the implementation of the Promotion of Access to Information Act: the Department of Justice, the Human Rights Commission, and the Government Communication and Information Service. There is no specialized enforcement body for the right of access to information, although advocates are pushing for such a mandate to be combined with a specialized body to enforce the privacy/data protection law currently early in the legislative drafting process.

Despite the organizational power of the South African military and intelligence bureaucracies, it does seem significant that their power has been at least partially exercised through legal forms. The preamble to the MISS is one example. That power has also been exercised under the shadow of a constitutional right of access to information backed by a judiciary with the power and will to enforce that right. It is remarkable that legislation restricting disclosure of information passed after the right to information law in South Africa has been careful to be consistent with the 2000 law.[45]

Conclusion

Elaine Scarry offers a piercing analysis of national security in the wake of September 11.[46] She argues for a citizen-focused version of national security. She points out that the only (apparently) successful defence of the four airplanes seized on that day was accomplished not by the F-15s deployed by the defence networks but rather by a group of the individuals aboard one of the airplanes. In her analysis of the event, a key feature is the rapid diffusion of information from and to the passengers on the airplane through the use of cellphones and on-board telephones. She concludes by arguing in favour of decentralized (citizenship-based) rather than centralized modes of national defence.[47]

This episode is relevant because it shows a direct relationship between a vision of citizenship and the concept of national security. Usually, the argument for greater information improving national security is made indirectly. In one indirect version, greater information accessibility entails greater accountability and thereby better national security. In another indirect version, greater information accessibility provides more and more accurate information to centralized military authorities who may then use that information to provide better national security. Elaine Scarry's analysis of the 11 September story shows the strong version of the argument in favour of a citizen's right to information. It shows at least one plausible episode where the benefit to national security is more than indirect.

---

[45] One example is the Financial Intelligence Centre Act.

[46] E Scarry 'Citizenship in Emergency: Can Democracy Protect Us Against Terrorism?' Boston Review (available at http://bostonreview.mit.edu/BR27.5/scarry.html).

[47] Tom Blanton's paper also alludes to this citizen defence example. See Blanton at 29-34. In this sense, I would agree with Blanton that one needs to go beyond the balance metaphor. The challenge would be to develop an information regime that both directly incorporates national security and directly incorporates the informational dimension of citizenship.

A final observation comes with the relaxation of the assumption of a military based definition of national security. When one starts to think of national security in an expanded sense, one of the most important of those senses in the South African context is the achievement of socio-economic rights.[48] These rights are guaranteed in the South African Constitution and have been enforced and found justiciable in a series of cases by the Constitutional Court of South Africa. The role that the right of access to information may play in the promotion and protection of socio-economic rights is only beginning to be explored.[49] For the achievement of this understanding of national security, the right of access to information is crucial. Furthermore, it is likely that the practices and concepts developed within the military field of national security will influence practices throughout the field of national information policy.

[48] It is of course possible to contest the definition of the concept "national security". One way might be to distinguish between military security, political security, and bureaucratic security. Another way is to use the term security for other policies and programmes than military ones. For instance, one can speak of food security. To this point, this paper has used a military definition of national security.

[49] See J Klaaren 'A Second Look at the Human Rights Commission and the Promotion of Socio-Economic Rights' (paper delivered at the South Africa Reading Group of New York Law School and the Constitutional Roundtable of the University of Toronto Faculty of Law) and R Calland and A Tilley (eds) The Right to Know, the Right to Live (2002). A recent case uses the constitutional right to information but not the AIA to order the government to hand over some documents related to the arms deal. See 'Govt given 10 days to hand over arms documents' Mail and Guardian (27 March 2003).