THE PROTECTION OF STATE INFORMATION BILL B6-2010, UNIVERSITIES AND ACADEMIC FREEDOM

Higher Education South Africa (HESA)

17 February 2012

Contact details:
Dr Jeffrey Mabelebele (Acting CEO)
Tel: 012 481 2842
Email: admin@hesa.org.za

EXECUTIVE SUMMARY AND RECOMMENDATIONS

The South African Constitution protects the right to academic freedom as part of freedom of expression. To enjoy this freedom, there is a need for free access to and dissemination of information. In spite of the fact that the Protection of State Information Bill has undergone many positive changes, the Bill still threatens these rights in various ways. Not only could the Bill potentially limit the ability of academics to engage in teaching and research on legitimate subjects, but it also threatens information flow in society generally about security matters. The concerns of Higher Education South Africa are not confined to the implications of the Bill for the activities of its own members, but we are concerned about its implications for society as a whole. Much of the public debate on the Bill has been about its likely effects on the media, with focus on its implications for academia, and for the academy – society interface. This paper addresses that gap.

The Bill will make research into aspects of the security cluster extremely difficult. Any research that is in the public interest, but that is based on leaked classified information, will be criminalised and the researcher could be arrested for failing to report possession of classified information. The Bill does penalise those who classify information for improper purposes, such as to conceal corruption or prevent embarrassment. However, there are many documents that may be classified for what the Bill considers to be 'proper reasons' that researchers will be unable to access, given the vague grounds for classification and still overbroad definition of national security (although these aspects of the Bill have been improved).

The declassification procedures are bound to frustrate even the most tenacious of researchers. Academics whose research depends on classified information would not be able to plan their research work easily since the period for determination of requests for classified information will be determined within an undefined 'reasonable time'. Researchers will now have to, in addition to researching for relevant information, confirm with classification authorities whether the information they gleaned from public sources are classified or not. Otherwise, they face an imprisonment term for obtaining, holding, releasing or publishing classified information. This will inevitably have a chilling effect on academic freedom. The possession or publication of classified material should not be criminalised, otherwise researchers may be put off from researching the security cluster for fear of coming into possession of a classified document.

Since the application, review and appeal for access to information in this area have been restricted to those officials and line ministers who classified the information in the first place, it would now be nigh impossible to obtain information especially on controversial projects that require review. The situation is not made easier by the fact that the Bill does not protect researchers who somehow manage to obtain the information from employees working in these areas. While the whistleblower is protected from prosecution for disclosure, the researcher is not and can face imprisonment for a term ranging from 5 years to 25 years depending on the type of information received/published.

Research into court proceedings and critiques of court judgments is made impossible especially in those cases where evidence and documents relied on by the courts in reaching their conclusions are classified. This is because courts are now precluded from enclosing this evidence in their judgments. A researcher who wishes to critique the conclusions of the judges would now have to apply to the relevant court for access to these classified evidences. The attendant cost and time makes this area a no-go zone for many, if not most, researchers.

Researchers and students from foreign countries could be exposed to unreasonable suspicion and intimidation by section 41 of the Bill, which makes it an offence to be an unregistered intelligence agent if you have the *potential* or *expectation* of being a foreign intelligent agent. If uncircumscribed, this provision could hamper international academic exchange and collaboration among scholars, and contribute to a drop in foreign-student/scholar applications to South African colleges and universities.

The implications of these provisions are that teaching and research on the security cluster will be frustrated. Several universities undertake research and offer courses on strategic studies, and they will be the most heavily affected. Researchers and lecturers may shy away from studying current issues concerning the security cluster, as the information needed to undertake this work may be difficult to access. They may also fear the dilemmas presented by coming into the possession of classified documents, including having to reveal sources of information that are necessary to undertake their research. Prospective interviewees could well dry up, as they fear disclosing confidential information.

These problems could lead to teaching and research becoming detached from the events taking place in the security cluster. Knowledge production about strategic issues facing the cluster, and the role of the police, intelligence sector and the military in society, will become more difficult. Universities have a role to play in democratising knowledge to improve society. If they cannot obtain access to the information necessary to generate this knowledge, then society will be the poorer for it.

A secretive security cluster, sealed up from public scrutiny, is dangerous. World history is littered with examples of intelligence officials, police and military personnel who have abused their power when secrecy prevails over transparency. Furthermore, if academics cannot access information about the cluster readily, then crucial lessons to be learned from problems that have arisen in the cluster cannot be analysed, which may deny the intelligence, military and police crucial opportunities to become learning organisations. A security cluster that is not informed by debate about its priorities and activities can quickly become inward focussing and out of touch with reality. It may fail to address key social problems, or it may address them inappropriately.

While we acknowledge that there is information that should be kept secret to protect national security – especially operational information – we feel that the Bill sets the bar for access to information far too low for our comfort.

RECOMMENDATIONS

The paper recommends numerous changes to the Bill to reduce the potential impact on academic freedom. These are as follows**:**

Definitions

- The list of components that comprise national security in the Bill should be made exhaustive so as to avoid introduction of new areas.
- Economic, scientific and technological information should not form part of the definition of national security or if they do they should be restricted to those specific matters that relate to national security and not merely vital to the Republic.

Scope of the Bill

- Limit the classification to state security organs without the opt-in clause. The opt-in clause would only encourage institutions hell-bent on hiding information to apply for the same.

General principles of state information

- This section should be redrafted to read: "paragraphs (a) to (i) are to be balanced against the security of the Republic, in that access to information should not be unduly denied."

Policies and procedures

- Delete clause 7 and make the national information security standards prescribed by the minister uniformly applicable to all organs of state.

Information which require protection against alteration, destruction or loss

- Define the level of "administrative control" that organs of state should exercise over valuable information, or include a proviso to the effect that the exercise of administrative control must not be used to frustrate access to valuable information.

Classification of information

- The classification criteria "demonstrable harm", "serious demonstrable harm" and 'serious or irreparable harm" need to be clearly defined or guidance given as to their meaning. In this regard, the Bill should ensure that the definitions or guidance adopted can allow for an objective demonstration of harm with a standard measure of reasonableness.
- The Bill should provide a requirement on the part of the classifying officer to give reasons in writing for classifying information or for classifying it in a certain category.
- Clause 13(5) which allows for the classification of entire categories of information even where only minimal amounts of information warrant classification should be deleted as it undermines the intentions and objective of the Bill and makes the bill unconstitutional.

Declassification of information

- In the interests of promoting access to information, regulated information should be classified for not more than 10 years, followed by renewals of up to 5 years
- The process of automatic declassification of apartheid-era classified documents, as was foreseen in the 2008 version of the Bill, should be restored.

Regular Reviews, Request for Access to Classified Information and Status Review

- Reviews of classification should be carried out at least once every 5 years.
- Once an application for information is made, the relevant authority should not take more than 30 days to arrive at a decision. The time period for requests revealing contravention of, or failure to comply with the law, should remain 14 days.
- Simplify and broaden the public interest override. In addition to information that reveals contravention, or failure to comply with the law; or an imminent and serious public safety or environmental risk, the public interest override should also apply to information that reveals risks to public health, defence and security, and international relations.
- Harmonise the Bill with the provisions of the Promotion of Access to Information Act, by requiring a request for access to classified information to be dealt with in terms of the latter Act.
- The composition and procedures of appointment of the Classification Review Panel should be revised to ensure its independence and impartiality.

Appeals

- Appeals against decisions of the heads of organs of state should be made to an independent arbitrator, probably, a retired judge.

Implementation and monitoring

- In order to encourage independent oversight and efficient implementation, we recommend a constitutional amendment creating an independent Chapter Nine institution with wide-ranging powers headed by a retired judge, to monitor the implementation of the Bill. All organs of state involved in the classification and declassification of state information should be subjected to the monitoring regime.

Offences and penalties

- The Bill should provide for a public interest defence crafted in a way that provides for extensive protection and broad applicability, as well asa public domain defence. The public interest defence should apply broadly to where the information reveals incompetence, negligence, criminality, illegality, corruption or hypocrisy on the part of government officials; or where the information reveals risks to the safety, health, security, or defence of the public; or where the public interest in receiving the information outweighs the harm in releasing it. On the other hand, the public domain defence should apply where the impugned information is already in the public domain.

Protection of information in courts

- The entire provision of clause 52 of the Bill should be amended to reflect the principle of open justice in that all documents placed before the court, whether classified or not, should be accessible to the public, unless a court, in the interest of justice, orders otherwise.

General provisions

- The Bill should repeal *all* inconsistent provisions in the existing statutes in order to align them with the new classification regime that it proposes.

1.0 The Protection of State Information Bill, Universities and academic freedom

Introduction

This paper unpacks some of the implications of the Protection of State Information Bill B6-2010 (5 September 2011) for academic freedom. Media attention has focussed on the implications of the Bill for journalists, with many media commentators expressing the view that if the Bill becomes law, then a great deal of investigative reporting would be criminalised. However, the implications of the Bill for academia and broader society are not well understood. This paper was commissioned by Higher Education South Africa (HESA), to inform universities about the Bill and its likely effect on academic freedom.

The Bill covers two types of information: valuable information and classified information. It will repeal the Protection of Information Act of 1982. The Bill had its genesis in a law reform process initiated in the mid 2000's, which gave rise to a Protection of Information Bill of 2008. This Bill was withdrawn and reintroduced in 2010.[1]

The Bill has been through a series of public hearing, as well as deliberations. In view of disagreements about fundamental aspects of the Bill, the ad-hoc committee that considered the Bill applied for an extension of 23 September 2011 to complete its work. The African National Congress (ANC) also made certain concessions to critics of the Bill on the 24 June 2011, and these concessions were debated in deliberations and incorporated, to an extent, into the Bill. Key concessions are as follows:

- All organs of state will not be required to classify information on national security grounds, but merely the organs of state security, with an opt-in clause for other organs of state.
- Minimum mandatory sentences in the Bill's penalties clauses have been dropped, with the exception of sentences that apply to espionage offences.
- An independent appeal mechanism for individuals who wish to appeal a classification decision must be included, and an independent classification review panel must be established to conduct oversight of the classification process.

[1] See Iain Currie and Jonathan Klaaren, Evaluating the Information Bills: a briefing paper on the Protection of Information Bill, paper produced on behalf of the Centre for Memory at the Nelson Mandela Foundation, 17 June 2011, 2-4.

The Bill was passed by the National Assembly on 22 November 2011, and referred to the National Council of Provinces for consideration.

This submission consists of two parts. Part A includes some general observations about academic freedom, as well as a clause by clause analysis of the Bill. **Part B** sets out details of research projects which may be affected by the regulation of access to information as proposed in the Bill. This paper has been compiled by Prof. Jane Duncan, Highway Africa Chair of Media and Information Society, Rhodes University, Dr. Rosaan Kruger, senior lecturer, Rhodes University Law Faculty, Rhodes University PhD candidate in the Law Faculty, Ken Obura and MA candidate in the School of Journalism and Media Studies Michelle Solomon.

PART A

2.0 Introduction

The founding values of the Republic of South Africa are set, amongst others, to include 'supremacy of the constitution and the rule of law' and democratic governance 'to ensure accountability, responsiveness and openness'.[2] Legislative regulation of the classification of information and access to such information must thus accord with these values, and more pertinently be in line with the constitutional rights relevant to the access of information.

Section 32 of the Constitution provides:

1. Everyone has the right of access to
    a. any information held by the state; and
    b. any information that is held by another person and that is required for the exercise or protection of any rights.
2. National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state

The legislation referred to in ss2 is the Promotion of Access to Information Act, 2000.

Section 16 of the Constitution reads:

1. Everyone has the right to freedom of expression, which includes
    a. freedom of the press and other media;
    b. freedom to receive or impart information or ideas;
    c. freedom of artistic creativity; and
    d. academic freedom and freedom of scientific research.
2. The right in subsection (1) does not extend to
    a. propaganda for war;
    b. incitement of imminent violence; or
    c. advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm.

These rights are not absolute in their functioning and they may justifiably be limited in terms of s 36 of the Constitution which provides:

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

[2] Section 1 of the Constitution of the Republic of SA, 1996.

based on human dignity, equality and freedom, taking into account all relevant factors, including

a. the nature of the right;
b. the importance of the purpose of the limitation;
c. the nature and extent of the limitation;
d. the relation between the limitation and its purpose; and
e. less restrictive means to achieve the purpose.

2. 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.

There is no doubt that the protection of valuable information from loss, destruction or alteration, and the classification of information concerning national security and the regulation of access thereto are constitutionally defensible. The question, however, is whether the scheme put forward in the Bill which limits the rights set out above, is constitutionally justifiable. In other words, are the rights of access to information and freedom of expression justifiably limited by the Bill and in accordance with the founding values set out above.

The paper analyses the Bill with a specific view of its impact on academic freedom. It is accordingly appropriate to comment on the meaning and scope of academic freedom and its relation to access to information.

3.0 Academic freedom

Section 16 (1) (d) of the Constitution provides that 'everyone has the right to freedom of expression, which includes ... academic freedom and freedom of scientific research.'[3] Some authors contend that the use of 'everyone' implies that the right to academic freedom applies only to academic scholars (teachers, researchers and students) and not to learning institutions.[4] However, as comparable jurisprudence from courts of other countries show, the right to academic freedom can also accrue as a collective right of the academic body, or as a corporate right of the university.[5] Such a position is not inconsistent with the Constitution, which allows juristic persons, such as universities, to enjoy 'the rights in the Bill of Rights to the extent required by the nature of the

[3] Constitution, s 16(1)(d).
[4] See Ian Currie & De Waal *The Bill of rights* (2005) 370 (arguing that the right vests in individual academics and not university).
[5] See, for example, *Sweezy v New Hampshire* 354 U.S. 234 (1957) at 262. In *Regents of the University of California v Bakke* 438 U.S. 265 (1978) at 312, the US Supreme Court defined "institutional academic freedom" as the freedom of the university to make its own judgment as to education. But see Ian Currie & Dewaal *The Bill of rights* (2005) 370 (arguing that the right vests in individual academics and not university).

rights and the nature of that juristic person.'[6] Indeed, this broad understanding of the subjects of the right to academic freedom fit the right's historical development in South Africa.[7]

The content of the right, however, defies absolute definition.[8] Nevertheless, many commentators today accept that it encompasses: 1) institutional autonomy from the state and other outside interference; and 2) a climate of free teaching, learning, criticism, and debate within a university.[9] The first element implies that the university should be free to determine for itself who may teach, what may be taught, how it shall be taught, and who may be admitted to study.[10] The second

---

[6] Constitution, s 8(4). In the *First Certification* case an objection was raised that, inconsistently with Constitutional Principle II, the extension of the rights guaranteed by the Bill of Rights to juristic persons would diminish the rights of natural persons. The Constitutional Court rejected the objection in the following terms:

> " . . . [M]any 'universally accepted fundamental rights' will be fully recognised only if afforded to juristic persons as well as natural persons. For example, freedom of speech, to be given proper effect, must be afforded to the media, which are often owned or controlled by juristic persons. While it is true that some rights are not appropriate to enjoyment by juristic persons, the text of NT 8(4) specifically recognises this. The text also recognises that the nature of a juristic person may be taken into account by a court in determining whether a particular right is available to such person or not."

See *Ex Parte Chairperson of the Constitutional Assembly: In Re Certification of the Constitution of the Republic of South Africa 1996* 1996 (10) BCLR 1253 (CC); 1996 (4) SA 744 (CC) at para 57.

[7] This past was characterised by state interference in the running of institutions of higher learning leading to the often quoted criteria for South African academic freedom set by Thomas Benjamin Davie. For Davie, academic freedom meant "our freedom from external interference in (a) who shall teach, (b) what we teach, (c) how we teach, and (d) whom we teach". See A van de Sandt Centilivres *Thomas Benjamin Davie, the first TB Davie Memorial lecture, delivered at the University of Cape Town on 6 May 1959* (1961) at 5.

[8] See, for example, C. Kaplan, & E. Schrecker, (eds.), *Regulating the Intellectuals: Perspectives on Academic Freedom in the 1980s,* (1983) at 6 (pointing out that 'there is little consensus regarding the meaning of academic freedom although there is agreement that it is something worth protecting"); C. Russell, *Academic Freedom,* (1993) at 1 (pointing out that 'academic freedom' has often caused confusion because it comes from a medieval intellectual tradition which pre-dates most of the current meanings of the word 'freedom'); N. Smith, 'Constitutional Academic Freedom', *South African Law Journal,* Vol. 112, No. 4, 1995, pp. 678-680, at p. 680.

[9] The South African National Commission on Higher Education, for example, asserts that the right to academic freedom is "the right to academic freedom for all individuals engaged in responsible academic work and the right to autonomy for higher education institutions in fulfilling their educational and academic roles." National Commission on Higher Education *A framework for transformation* (1996) at 196-197. See also Fuchs "Academic Freedom – Its Basic Philosophy, Function, and History" (1963) 2 *Law & Contemp. Probs.* 431. At 431 Fuchs States:

> Academic freedom is that freedom of members of the academic community, assembled in colleges and universities, which underlies the effective performance of their functions of teaching, learning, practice of the arts, and research. The right to academic freedom is recognized in order to enable faculty members and students to carry on their roles.

See also Machlup "On some Misconceptions Concerning Academic Freedom" (1955) 41 *AM. A.U. Professors Bull* 753. At page 753-754 Machlup states

> Academic freedom consists in the absence of, or protection from, such restraints or pressures, chiefly in the form of sanctions threatened by state or church authorities or by the authorities, faculties, or students of colleges and universities, but occasionally also by other power groups in society – as are designed to create in the minds of academic scholars (teachers, research workers, and students in colleges and universities) fears and anxieties that may inhibit them from freely studying and investigating whatever they are interested in, and from freely discussing, teaching, or publishing whatever opinions they have reached.

[10] In *Sweezy v New Hampshire* 354 U.S. 234 (1957) at 263 the court quoted with approval the statement of a conference of senior scholars from South African universities which concluded:

> It is the business of a university to provide that atmosphere which is most conducive to speculation, experiment and creation. It is an atmosphere in which there prevail "the four essential freedoms" of a

element, on the other hand, implies that individual academics should be free to research, teach, and learn without undue interference, censure or obstacles.[11] This, of course, does not mean that the freedom can be used irresponsibly.[12] On the contrary, academic freedom comes with responsibilities, among which, are observance of scholarly ethics[13] and a dedication to and understanding of an academic freedom that one extends as freely to others as to oneself.[14]

To enjoy this freedom, there is need for free access to and dissemination of information.[15] Free flow of information engenders an atmosphere of openness, which enables academics to achieve their goals and the society to benefit from the results of research.[16] Openness allows an academic not only to access information for research and generate knowledge but also to freely debate and disseminate the ideas, ideologies and findings to fellow academics, the public and the government.[17] The resultant flow of information also helps to hold academics publicly accountable for their work and to develop well-informed public policy. The Constitutional Court has recognised this link

---

> university – to determine for itself on academic grounds who may teach, what may be taught, how it shall be taught, and who may be admitted to study.

This holding on the institutional autonomy of the universities was approved by Justice Powell in *Regent of the University of California v Bakke* 438 U.S. 265 when in announcing the Courts judgment held that the selection of its student body was within the freedom of a university to make its own judgments.

[11] See, for example, Department of Education *Programme for higher education transformation* (1997) at 7 ("The principle of academic freedom implies the absence of outside interference, censure or obstacles in the pursuit and practice of academic work. It is a precondition for critical, experimental and creative thought and therefore for the advancement of intellectual inquiry and knowledge"). See also Van Alstyne "The Specific Theory of Academic Freedom and the General Issue of Civil Liberties" (1972) 404 *Annals 140 at 146:*

> The phrase "academic freedom" in the context "the academic freedom of a faculty member of an institution of higher learning," refers to a set of vocational liberties: to teach, to investigate, to do research, and to publish on any subject as a matter of professional interest, without vocational jeopardy or threat of other sanction, save only upon adequate demonstration of an inexcusable breach of professional ethics in the exercise of any of them.

[12] Certainly, it would be an unwarranted expansion of academic freedom to, for example, permits a claim of institutional academic freedom to impair the ability of claimants to prove sex and race discrimination in tenure and promotion decisions. Such was the case in *re Dinnan* 661 F.2d 426, 432 (5th Cir. 1981) (where the US Court held that academic freedom cannot be used to avoid responsibility for one's action).

[13] These require that in the process of following ones ideas, arguments, insights and findings, one must avoid such misconduct as plagiarism, falsification of data and unethical research practice.

[14] As Francis Bacon noted in his *The Novum Organum The New Instrument of Knowledge* (1863) 59-60:

> We are so prone to error: from the limits of human powers; from individual bias; from the equivocation of our words; from the inveterate flaws of those inherited human theories that we take as nature's own. To overcome these propensities for self-deception and illusion, we need to guard, above all, against those things we wish to believe, to devise tests of precisely the hypotheses to which we are drawn, and, an essential part of true academic freedom, to encourage the presence of those who disagree with us, even indeed, above all sharply.

[15] As the Protection of Information Bill recognizes at s 6, "accessible information builds knowledge and understanding and promotes creativity, education, research, the exchange of ideas and economic growth".

[16] The core role of higher learning institutions is to carry out research, and present findings to fellow academics, the public and the government. Free flow of information makes this possible as it promotes innovation and discovery.

[17] As the Academy of Science of South Africa correctly points out, academic freedom cannot be realized "without the exercise of the freedom to research, write, and speak robustly and professionally, without fear or favour on any topic including the impact of science on society." "Academic Freedom Statement from the Academy of Science of South Africa" April 6 2010 http://www.assaf.org.za/2010/04/academic-freedom-statement-from-the-academy-of-science-of-south-africa-assaf/

between free flow of information and the enjoyment of freedom of expression, of which academic freedom is part.[18] In *Brummer v Minister for Social Development and Others*[19] the Court stated that '… access to information is crucial to the right to freedom of expression which includes freedom of the press and other media and freedom to receive or impart information or ideas'.[20]

Albert Einstein aptly noted:

> 'By academic freedom I understand the right to search for the truth and to publish and teach what one holds to be true. This right also implies a duty; one must not conceal any part of what one has recognized to be true. It is evident that any restriction of academic freedom serves to restrain the dissemination of knowledge, thereby impeding rational judgment and action'.[21]

Scholarly analyses of current events and policies enrich public discussion, ensure accountability and transparency in governance and open up new possibilities for policy formulation and governance. This need for free flow of information in academic freedom lies in the understanding that the society benefits when academics are able to search for truth without external hindrance and when they are able to report their findings regardless of what those findings may be.[22] Such an understanding recognises that knowledge is never neutral, never pre-existent, and never 'up for grabs' and that only by accessing information, analysing that information and presenting the findings can academics help the society to develop in an informed direction.[23] It is thus imperative that access to information be in line with the constitutional provisions set out above.

In what follows, the provisions of the Bill are considered for their constitutional compatibility, specifically in relation to academic freedom.

---

[18] In fact academic freedom is provided for as a subset of the freedom of speech. See Constitution, art 16.
[19] CCT 25/09) [2009] ZACC 21; 2009 (6) SA 323 (CC) ; 2009 (11) BCLR 1075 (CC) (13 August 2009)
[20] Above, para 63 (footnotes omitted)
[21] Albert Einstein, quotation inscribed on his statute in front of the National Academy of Sciences, Washington, DC. See Academic Freedom Statement from the Academy of Science of South Africa, (pointing out that it is only "through high-quality teaching and research, in a climate of academic freedom and social responsiveness, that higher education best fulfils its accountability to society").
[22] As American Association of University Professors have noted," Institutions of higher education are conducted for the common good and not to further the interest of either individual teacher or the institution as a whole. The common good depends upon the free speech for truth and its free exposition. Academic freedom is essential to these purposes." See AAUP "Academic Freedom and Academic Tenure" 1940/1977.
[23] For more, see WG Tierney and VM Lechuga "Academic Freedom in the 21st Century" (2005) *Thought and Action* 7

4.0 Introduction

This second limb of the research on the effect of the Bill on academic freedom gives a detailed analysis of each chapter of the Bill. It notes at the outset that the revised Bill has made some positive improvements. Overall it is more concise and coherent. There are also now strong guidelines on the type of information that should be protected. However, many of the fundamental issues that have a bearing on access to information, which, as demonstrated in the first paper, is crucial to the enjoyment of academic freedom, remain unchanged. The analysis seeks to highlight these areas and provide some considered suggestions on how to remedy the identified shortcomings in the bill.

5.0 Definitions, Objects and Application of the Bill

5.1 Objects

The Bill lists 12 specific objects which it aims to achieve.[24] In a nutshell it proposes to replace the 1982 Protection of Information Act with a new open statutory framework.[25] The statutory framework it proposes to establish is for the protection of State information against unlawful alteration, destruction or loss and for classifying, preserving and declassifying state information so as to regulate access to all information in the hands of the state.[26] As the Memorandum on the Objects of the Protection of State Information Bill to the September 2011 Bill states:

> The Protection of State Information Bill (the Bill) will ensure a coherent approach to the protection of valuable information and the classification and declassification of state information. It will create a legislative framework for the state to respond to espionage and other associated hostile activities. [27]

We do not contest the objectives of the Bill or the need for a comprehensive Bill of this nature. We accept that given the complexities of modern government, situations do arise from time to time in which access to state information needs to be limited in order to protect the interest of the state and to ward off genuine threats to the nation's security. Our recurrent assertion, however, is that while certain information must be exempt from immediate disclosure for a number of distinct reasons, the overriding premise of the Bill should reflect that public records and information are the property of South African citizens, and all initial presumptions should favour disclosure.

---

[24] Section 2.

[25] The Bill was proposed to deal with "inconsistencies and discrepancies" within this Act. Amongst others, the Act was seen to be outdated in that it contained provisions perceived as being contrary to the Constitution. The Act was also weak in terms of providing sufficient protection for the state against information peddlers and spy activity. See *explanatory summary of Bill published in Government Gazette No. 32999 of 5 March 2010*

[26] Section 2

[27] See Memorandum on the Objects of the Protection of State Information Bill

This basic premise in the context of access to information has been upheld by the courts in a number of cases. For instance, in *Mthembi-Mahanyele v Mail & Guardian Ltd*,[28] Lewis JA held:

> The State and its representatives, by virtue of the duties imposed upon them by the Constitution, are accountable to the public. The public has the right to know what the officials of the State do in discharge of their duties.[29]

Similarly, in *Transnet Ltd v SA Metal Machinery Co (Pty) Ltd*[30] Heher JA held:

> [Transnet Ltd] being an organ of State, is bound by a constitutional obligation to conduct its operations transparently and accountably. Once it enters into a commercial agreement of a public character like the one in issue … the imperative of transparency and accountability entitles members of the public, in whose interest an organ of State operates, to know what expenditure such an agreement entails.[31]

In the case of *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services*,[32] Sachs J summarized the value of openness in the following immutable words:

> An open and democratic society does not view its citizens as enemies. Nor does it see its basic security as being derived from the power of the state to repress those it regards as opponents.[33]

In *Azanian Peoples Organisation (AZAPO) and Others v President of the Republic of South Africa and Others*[34], Mohamed DP justified this need for openness in the South African context thus: "secrecy and authoritarianism have concealed the truth in little crevices of obscurity in our (South African) history."[35]

In summary, we submit that the Bill must live to this basic premise of openness if it is to stand the test of constitutionality.

5.2 Definitions

The Bill under clause 1 provides for definitions of a number of terms used in the subsequent clauses of the Bill. Some of these definitions are discussed below. In analysing the definitions, we bear in mind the principle of legality under the South African Constitution, which requires that all laws be clear, precise and accessible.[36] While the principle has been interpreted as not requiring absolute certainty in meaning,[37] it, nevertheless, demands that laws be drafted with sufficient precision to

---

[28] 2004 (6) SA 329 (SCA)
[29] Para 66.
[30] 2006 (6) SA 285 (SCA)
[31] Para 55; further see *Intertrade Two (Pty) Ltd v MEC for Roads and Public Works, Eastern Cape* 2007 (6) SA 442 (C) at para 4; *South African Broadcasting Corporation v National Director of Public Prosecutions* 2007 (1) SA 523 (CC) at para 28.
[32] 2008 (4) SA 31 (CC) ("the Masetlha case").
[33] At para 155.
[34] [1996] ZACC 16; 1996 (4) SA 671 (CC); 1996 (8) BCLR 1015 (CC)
[35] at para 17.
[36] *Pharmaceutical Manufacturers Association of SA and Another: In re Ex parte President of the RSA and Others* 2000 (2) SA 674 (CC) at para 39; *De Reuck v Director of Public Prosecutions, Witwatersrand Local Division, and Others* 2004 (1) SA 406 (CC) at para 57; *Masiya v Director of Public Prosecutions, Pretoria and Another* 2007 (5) SA 30 (CC) at para 69
[37] *R v Pretoria Timber Co (Pty) Ltd & Another* 1950 (3) SA (A) 163 at 176G.

enable those to whom they are directed to have reasonable certainty about the conduct that is required of them.[38]

We also bear in mind the related principle of proportionality, which requires that the means employed in the law must be proportionate to the law's constitutionally legitimate underlying objectives. In this regard, laws that prohibit with the same stroke both constitutionally legitimate and illegitimate activity, are generally regarded as being overbroad and therefore unconstitutional. As Mokgoro J stated in *Case v Minister of Safety and Security; Curtis v Minister of Safety and Security*:[39]

> To determine whether a law is overbroad, a court must consider the means used … in relation to its constitutionally legitimate underlying objectives. If the impact of the law is not proportionate with such objectives, that law may be deemed overbroad.[40]

Has the definitions in the Bill met the requirements of these standards? We analyse some of these definitions in the following sub-sections.

5.2.1. "Information"

The definition of information is important as it influences the understanding of all the other definitions in the Bill relating to information. Information is defined as:

> any information contained in any document whether written, copied, drawn, painted, printed, filmed, photographed, magnetic, optical, digital, electronic or any other type of recording, measure, procedure, object or verbal announcement;

It is our view that this definition of "information" is now acceptable. Unlike the 2010 draft, it leaves out information that has not been reduced to material form out of its breadth.[41]

5.2.2 National Security

The Bill defines "sensitive information" as information that must be protected from disclosure in order to prevent the *national security* of South Africa from being harmed. This definition is

---

[38] *Affordable Medicines Trust and Others v Minister of Health and Others* 2006 (3) SA 247 (CC) at para 108. See also *De Reuck v Director of Public Prosecutions, Witwatersrand Local Division* 2004 (1) SA 406 (CC) at para 57.

[39] 1996 (3) SA 617 (CC)

[40] At para 49

[41] See Clause 1 of the 2010 Bill defined information as

> any facts, particulars or details of any kind, whether true or false, and contained in any form, whether material or not, including, but not limited to—
> (a) documents, records, data, communications and the like, whether in paper, electronic, digital, audio-visual format, DVD, microform C, microphone, microfilm and microfiche form or format or any other form or format; and
> *(b)* conversations, opinions, intellectual knowledge, voice communications and the like not contained in material or physical form or format;

important because it is only state information that qualifies as sensitive information that can be classified according to the Bill. Unlike the 2010 draft, "National security" is now more adequately described.[42] It is defined as including

> the protection of the people of the Republic and the territorial integrity of the Republic against—
> *(a)* the threat of use of force or the use of force;
> *(b)* the following acts:
> (i) Hostile acts of foreign intervention directed at undermining the constitutional order of the Republic;
> (ii) terrorism or terrorist related activities;
> (iii) espionage;
> (iv) exposure of a state security matter with the intention of undermining the constitutional order of the Republic;
> (v) exposure of economic, scientific or technological secrets vital to the Republic;
> (vi) sabotage; and
> (vii) serious violence directed at overthrowing the constitutional order of the Republic;
> *(c)* acts directed at undermining the capacity of the Republic to respond to the use of, or the threat of the use of, force and carrying out of the Republic's responsibilities to any foreign country and international organisations in relation to any of the matters referred to in this definition, whether directed from, or committed within, the Republic or not,
> but does not include lawful political activity, advocacy, protest or dissent;

This new definition of national security is a positive improvement in bringing the definition in line with the best practices worldwide. For example, in Lithuania, a state secret is limited to information that would "violate the sovereignty of the Republic of Lithuania, defence or economic power, pose harm to the constitutional system and political interests of the Republic of Lithuania, and pose danger to the life, health and constitutional rights of individuals."[43] Similarly, The US 2009 Executive Order on Classification sets out eight areas that are eligible for classification as:

- Military plans, weapons systems, or operations;
- Foreign government information;
- Intelligence activities (including special activities), intelligence sources or methods, or cryptology;
- Foreign relations or foreign activities of the US, including confidential sources
- Scientific, technological or economic matters relating to national security which include defence against trans-national terrorism;
- US government programs for safeguarding nuclear materials or facilities;
- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans or protection services relating to national security, which includes defence against transnational terrorism;
- Weapons of mass destructions

However, while we recognize the improvement in the definition, we submit, that the list in the Bill should be made exhaustive so as to avoid introduction of new areas during application. This requirement for specificity in the definition of national security in secrecy laws has been recognized

---

[42] The 2010 version defined National Security at clause 1 as:

> The resolve of South Africans as individuals and as a nation to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life, and includes protection of the people and occupants of the Republic from hostile acts of foreign intervention, terrorism and related activities, espionage and violence, whether directed from, or committed within, the Republic or not, and includes the carrying out of the Republic's responsibilities to any foreign country in relation to any of the matters referred to in this definition.

[43] For a discussion, see Miklós Harszti, *Access to information by the media in the OSCE region: trends and recommendations. Summary of preliminary results of the survey* Vienna, 30 April 2007

both locally and globally. For example, the *Johannesburg Principles on National Security, Freedom of Expression and Access to Information,* which was adopted on 1 October 1995 by an international group of experts in human rights, national security and international law, states in principle 2(a) that:

> A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.[44]

In Principle 12 it directs that a government must designate "only those *specific* and *narrow categories* of information that it is necessary to withhold in order to protect a legitimate national security interest"[45] (Emphasis ours).

We further submit that economic, scientific and technological information should not form part of the definition of national security or if they do they should be restricted to those specific matters that relate to national security and not merely vital to the Republic.[46] This would be in line with the condition in section 14(h) of the Bill, which provides that "scientific and research information not clearly related to national security may not be classified". It would also avoid unjustified infringement on the right to access to information and freedom of expression. The Human Rights Committee, the body charged with interpreting and overseeing the implementation of the International Convention on Civil and Political Rights (ICCPR), has held, for example, that issues related to science, banking and commercial sector should not form part of restricted information under national security as their inclusion would unjustifiably infringe on individual rights especially the right to freedom of expression (of which academic freedom is part).[47]

1.1.1. State Security Matter

The definition of "State security matter" is also of importance as the disclosure of information that amounts to state security matter is considered by the Bill as a criminal offence punishable by a maximum of 15 years imprisonment.[48] This term is defined in the Bill as including:

> [A]ny matter, which has been classified in terms of this Act and, which is dealt with by the Agency or which relates to the functions of the Agency or to the relationship existing between any person and the Agency.[49]

---

[44] Principle 2(a)
[45] Principle 12
[46] See Protection of State Information Bill, s 1(b)(v)
[47] Human Rights Committee, *2001 Concluding Observations on Uzbekistan's State Report* Available at http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/CCPR.CO.71.UZB.En?Opendocument (Accessed on 9 June 2010).
[48] Protection of State Information Bill, s 49
[49] Protection of State Information Bill, s 1

We submit that this definition is now defensible as it now limits State Security Matter to only those matters that have been classified. This is unlike the 2010 draft which brought within its ambit information which was not necessary classified. The 2010 draft defined State Security Matter as:

> [A]ny matter which is dealt with by the Agency or which relates to the functions of the Agency or to the relationship existing between any person and the Agency

1.2. Application of the Bill

Section 3 provides that the Bill applies to all organs of state with regard to protection of valuable information. With regard to classification, reclassification and declassification the Bill is made applicable only to security organs and oversight bodies. However, the minister in charge of security has been reserved the right, upon application by interested organ of state, to allow that organ to classify information.

We submit that the opt-in clause that allows any organ of state that wants to classify information to apply for the power of classification if they can show good cause could be amenable to abuse. This is because the provision does not provided for the criteria for granting permission – good cause, in our view, is too broad in that it might cover anything.

Recommendation: Limit the classification to state security organs WITHOUT the opt-in clause. The opt-in clause would only encourage institutions hell-bent in hiding information to apply for the same.

2.0. Chapter 2: General Principles of State Information

Clause 6 of the Bill identifies 10 principles that underpin and inform the implementation and interpretation of the Bill. It recognises access to information as a right and states that free flow of information "promotes openness, responsiveness, informed debate, accountability and good governance".[50] In this regard, the section instructs that all measures taken in accordance with the Bill must have regard to the Bill of Rights, specifically the right to freedom of expression and the right to access to information.[51]

[50] Section 6 (c) & (d)
[51] Section 6(i)

These principles are an attempt to synchronize the Bill with the South African constitution, which contemplates a South African society that is open and accountable.[52] The Constitution requires that "[t]ransparency must be fostered by providing the public with timely, accessible and accurate information."[53] This open and transparent regime has been given effect to and is now regulated by the South Africa's right-to-information laws, namely; the Promotion of Access to Information Act No. 2 of 2000, the Promotion of Administrative Justice Act No. 3 of 2000 and the Protected Disclosures Act No. 26 of 2000.

We commend the drafters for acknowledging these principles. However, it is our view that Principle j which allow for all other information principles to be trumped by 'national security' spoils the whole section and makes it arguably unconstitutional. The principle provides that when considering whether to classify information the deciding person must have due regard to the security of the Republic, in that "the national security of the Republic may not be compromised."[54] What this means is that classification of document should always trump when there is any uncertainty. In other words, the fall-back position is to classify as opposed to declassify. Such a clause has the potential of returning the country to the dark, secretive past.

This shift in favour of "national security" also betrays both the South African democratic commitment to openness and the Constitutional concept of national security as envisaged in section 198 (a) and (c). The section provides the "governing principles" for "national security" as follows:

> (a) National security must reflect the resolve of South Africans, as individuals and as a nation, to live as equals, to live in peace and harmony, to be free from fear and want and to seek a better life"….
> and
> "(c) National security must be pursued in compliance with the law, including international law."

We submit that Section 198(a) and (c) requires that national security be subjected to both "public benefit" and legal regulation. Principle j makes the Bill fall foul of this express Constitutional provision as it concretizes "national security" as an overriding right and makes decisions on national security a matter of discretion, as opposed to requirement of law.

Recommendation: We recommend that the wording of clause 6(j) be redrafted to read: "paragraphs (a) to (i) are to be balanced against the security of the Republic, in that access to

---

[52] Constitution, s 195(1)(f).
[53] Constitution, s 195(1)(g). The Constitutional Court stressed this point in *Brummer v Minister for Social Development and Others* when it said: The importance of the right to access to information, in a country which is founded on values of accountability, responsiveness and openness, cannot be gainsaid. Id para 62.
[54] Protection of State Information Bill, s 6 (j).

information should not be unduly denied." This latter proposal is in line with the ruling of Sachs J in *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services*,[55] where he, with respect, rightly stated:

> In answering [the question of whether documents should be redacted and then released to the public], it is important not to deal with hypothetical damage that could be caused to national security if certain types of information were to be revealed, but rather to verify whether on the facts a real risk exists that non-trivial harm could result. *More particularly, it has to be asked whether more harm could well result from disclosure than from non-disclosure* (our emphasis). [56]

3.0. Chapter 3: Policies and procedures

Clause 7 gives heads of states the power to come up with policies, directives and categories for classifying, downgrading and declassifying state information and protection against alteration, destruction or loss of state information created, acquired or received by that organ of state. Clause 7(3) provides that the policies and directives must not be inconsistent with the national information security standards prescribed by the minister.

It is our view that, in spite of the proviso in clause 7(3), clause 7 is unconstitutional as it creates uncertainty in the classification regime and as it denies effective public participation in the crafting of information security standards and procedures. First, given the fact that there are over 1000 organs of state in the Republic, [57] endowing each organ of state with the power to come up with its own distinct access policies, directives and criteria would create unjustifiable confusion and uncertainty on the access to information regime. Second, since the organs of state are not obliged to consult members of the public before coming up with the policies, citizens would be unjustifiably denied the right to participate in decisions that affect them. As observed by the Constitutional Court in *Premier of Mpumalanga v Executive Committee of the Association of governing Bodies of State-Aided Schools: Eastern Transvaal*:[58]

> Citizens are entitled to expect that government policy will ordinarily not be altered in ways which would threaten or harm their rights or legitimate expectations *without their being given reasonable notice of the proposed change or an opportunity to make representations to the decision maker* (emphasis ours).[59]

Recommendation: Delete clause 7 and make the national information security standards prescribed by the minister uniformly applicable to all organs of state.

4.0. Chapter 4: Information which require protection against alteration, destruction or loss

---

[55] 2008 (4) SA 31 (CC)
[56] Para 93
[57] The Institute for Democracy in Africa (IDASA) has identified over 1001 organs of state, which include an estimated 600 to 700 state owned entities. Available at http://www.idasa.org/media/uploads/outputs/files/schedule_of_organs.pdf.
[58] 1999 (2) SA 91 (CC)
[59] At para 41

Chapter 4 of the bill provides for the protection of state information against alteration, destruction or loss.[60] The state information which requires protection "against unlawful alteration, destruction, or loss" is described as "valuable information".[61] Valuable information is not defined in the Bill and is left for the regulation to be prescribed by the minister to define.[62]

Once information is identified as valuable, it need not be specifically marked, but holders of such information must be made aware of the need for controls and protections.[63] All individual items of information categorized as valuable are automatically deemed valuable.[64]

Valuable information is available and accessible to all persons and does not enjoy protection from unlawful disclosure.[65] However, such information is subject to administrative control and are to be handled with due care in accordance with procedures to be prescribed in regulations.[66] The Bill makes the destruction of public records subject to the National Archives and Records Service of South Africa Act, 1996.[67]

We accept that state information needs to be protected. However, we believe that this chapter as drafted allows for loopholes that can be exploited to frustrate access to information. Firstly, the Bill does not define "administrative control" leaving it to the organ of state to determine its contours. This is risky as institutions can opt to erect unnecessary bureaucracy on the way of access to valuable information. Secondly, there seems to be a conflict between the Bill and the National Archives and Records Service Act on whom between the National Archivist and organs of state has the final authority for the protection and management of valuable information. The Bill bestows the authority to protect and manage valuable information on the state organ,[68] while the National Archives Act bestows that authority on the National Archivist.[69] This conflict in duties might result in loss of valuable information as it becomes difficult to hold one entity accountable. This defect is

[60] Protection of State Information Bill, s 5 and 8
[61] Protection of State Information Bill, s 5.
[62] Protection of State Information Bill, s 1 & 8
[63] Protection of State Information Bill, s 9(2).
[64] Protection of State Information Bill, s 8(2)
[65] Protection of State Information Bill, s 5.
[66] Protection of State Information Bill, s 8.
[67] Protection of State Information Bill s 9(3). The National Archives Act aims to provide for, among other things, the proper management and care of the records of governmental bodies.[67] It creates the National Archivist and charges it with the management and care of public records in the custody of governmental bodies. The Act provides that no public record under the control of a governmental body shall be destroyed, erased or otherwise disposed of without the written authorisation of the National Archivist. National Archives Act, title, art 13(2)(a).
[68] National Archives Act s 9
[69] National Archives Act s 4 & 13

not cured by section 1(4) which only makes the Bill overriding in cases where there is a conflict in respect of *classified* information.[70]

Recommendations (1): Define "administrative control" or include a proviso to the effect the exercise of administrative control must not be used to frustrate access to valuable information. This is important given the background of a long history of abuse of governmental power in South Africa.[71] As the Constitutional Court stated in *Dawood v Minister of Home Affairs*:

> It is an important principle of the rule of law that rules be stated in a clear and accessible manner. It is because of this principle that section 36 [of the Constitution] requires that limitations of rights may be justifiable only if they are authorised by law of general application. Moreover, *if broad discretionary powers contain no express constraints, those who are affected by the exercise of the broad discretionary powers will not know what is relevant to the exercise of those powers or in what circumstances they are entitled to seek relief from an adverse decision* (emphasis added).[72]

Recommendations (2): Synchronize the Bill with National Archives and Records Service Act – in our view the responsibility for protection of valuable information should be singularly assigned to the respective organ of state as they are more conversant with the kind of information in their possession and are therefore in a better position to be held accountable for their protection.

5.0. Chapter 5: Classification and declassification of information

5.1. Classification

In addition to valuable information, the Bill also protects "classified information".[73] Classified information is described as "state information in material or documented form which requires protection against unlawful disclosure".[74] For state information to qualify for classifications it must be sensitive information, the release of which would harm the security of the nation.[75]

Initially the Bill included personal information, which was deemed to endanger the physical security or life of a person[76] and commercial information, which was outside the public domain and which if released publicly would cause financial loss or competitive or reputational injury.[77] These have, however, been left out.

---

[70] Protection of State Information Bill, s 1(4)
[71] For a discussion, see Richard Abel *Politics by Other Means* (1995)
[72] 2000 (3) SA 936 (CC), at para 47
[73] Protection of State Information Bill, s 5(2)
[74] Protection of State Information Bill, s 10
[75] Protection of State Information Bill s 1 and 10
[76] Protection of Information Bill 2010, s 15
[77] See report of Ad hoc committee on protection of information legislation on the Protection of Information Bill

The Bill provides that state information may be classified into three categories depending on the level of sensitivity. The first and least sensitive category is confidential information, where unlawful disclosure may cause "demonstrable harm" to national security.[78] The second category is secret information, where unlawful disclosure may cause "serious demonstrable harm" to national security.[79] The last and most sensitive category is top secret information, where unlawful disclosure may cause "serious or irreparable harm" to national security.[80]

Once information is classified, it becomes protected from unlawful disclosure and against alteration, destruction and loss.[81] All individual items of information that fall within the classified information are also deemed classified.[82] Classified information may only be accessible to those "holding an appropriate security clearance"[83] and those with "a legitimate need to access the information in order to fulfil their official duties or contractual responsibilities".[84]

The Bill also now provide for conditions for classification in clause 14. For example, under clause 14(b) classification may not be used to conceal illegality or administrative error. Clause 14(c) makes classification an exceptional exercise and 14(d) requires that it only be done when there is: "a clear, justifiable and legitimate need to do so; and a demonstrable need to protect the state information in the interest of national Security."

We commend the drafter for these conditions, which now provide strong guidelines on the type of information that should be protected. We still, however, have a number of concerns on the classification regime provided by the Bill. Firstly, the criteria for classifying material as "confidential", "secret" and "top secret" are still overbroad and vague. They unjustifiably leave the determination as to what information may be classified at what level to the subjective discretion of the classifying officer. For example, how accurately and objectively can a distinction be made between what is "demonstrable harm", "serious demonstrable harm" and 'serious or irreparable harm" to national security as to justify classification of information into "confidential", "secret" and "top secret" category? Related to this concern is the fact that the term "demonstrable harm" sets no

---

[78] Protection of State Information Bill, s 12(1).
[79] Protection of State Information Bill, s 12(2).
[80] Protection of State Information Bill, s 12(3)
[81] Protection of State Information Bill, s 10
[82] Protection of State Information Bill, s 13(5).
[83] [83] Protection of State Information Bill s 10. "Security clearance" is defined as a "a certificate issued to a candidate after the successful completion of a security screening investigation, specifying the level of classified information to which the candidate may have access subject to the need to know". Protection of Information Bill, s 1.
[84] [84] Protection of State Information Bill s 10. "legitimate interest" means an interest that is consistent with the Constitution, applicable law and the mandate of an institution or organ of state

lower limit on the probability of harm making it possible for something that has only a very remote chance of causing harm to qualify for classification.

Secondly, the Bill does not oblige decision makers to provide reasons for classifying information or for classifying it in a certain category. This means that decision makers cannot be made accountable for their decisions as the public or those supervising them would have no way of knowing whether a rational decision was made or not.

Thirdly, we submit that the requirement under clause 13(5) that all documents and information fall to be classified automatically once they form part of a certain category of information is not a proportionate restriction on the constitutional right of access to information. This is because a category in which, for example, only 1% of information is truly sensitive will erroneously permit the classification of the other 99%.

Recommendation (1): The term "demonstrable harm", "serious demonstrable harm" and "serious or irreparable harm" need to be clearly defined or guidance given as to their meaning. In this regard, the Bill should ensure that the definitions or guidance adopted can allow for an objective demonstration of harm with a standard measure of reasonableness.

This requirement for objectivity and reasonableness in the demonstrability of harm has been upheld in a number of cases by the courts. For example, in *S v Mamabolo*,[85] the Constitutional Court, when evaluating an allegedly scandalizing statement, insisted on *"an objective test, applied with the standard measure of reasonableness"* (emphasis added).[86] In that case the Court adopted the test for scandalizing as "whether the offending conduct, viewed contextually, really was likely to damage the administration of justice". [87]

With respect to the classification of information in the national security context, it is our view that the appropriate harm test articulated by Sachs J in *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services*[88] should be adopted:

> In answering [the question of whether documents should be redacted and then released to the public], it is important not to deal with hypothetical damage that could be caused to national security if certain types of information were to be revealed, but rather to verify whether on the facts a real risk exists that *non-trivial harm could*

[85] 2001 (3) SA 409 (CC).
[86] At para 43.
[87] At para 45.
[88] 2008 (4) SA 31 (CC).

> *result. More particularly, it has to be asked whether more harm could well result from disclosure than from non-disclosure* (emphasis added).[89]

The requirement of this test espoused by Sachs J, in our view, is that the classifying officer should not only satisfy himself/herself that the harm to national security is demonstrable but also that it is *non-trivial.* In addition, the classifying officer must also satisfy himself/herself that classification is the *best* possible way of dealing with the identified harm.

The proposal for the harm to be both demonstrable and non-trivial is not novel as it had been recognized by the 2010 under clause 21(1) in regard to decisions by classifying authority on whether to continue the classification of information or not. In this context, the 2010 Bill provided the test as whether the declassification "is likely to cause *significant* and demonstrable harm to the national security" (emphasis added).[90] We see no reason why the non-trivial requirement should not also be included at the first stage of classification.

Similarly, the requirement that classification should only be resorted to if it is the *best* option to dealing with the identified harm has also received support in other jurisdictions. For example, in the case of *New York Times Company v United States*,[91] where the United States government sought an injunction preventing the *New York Times* and the *Washington Post* from publishing excerpts from a classified historical study on the Vietnam war on the basis that the publication would endanger national security, the US Supreme Court held as follows:

> The entire thrust of the Government's claim throughout these cases has been that publication of the material sought to be enjoined "could", or "might", or "may" prejudice the national interest in various ways. But the First Amendment tolerates absolutely no prior judicial restraints of the press predicated upon surmise or conjecture that untoward consequences may result. … Thus, only government *allegation and proof that publication must inevitably, directly, and immediately cause the occurrence of an event kindred to imperilling the safety of a transport already at sea can support even the issuance of an interim restraining order* (Emphasis added).[92]

Indeed, there are many instances where disclosure of information that is potentially harmful to national security could be more helpful in addressing the identified harm than would be possible if the information was classified. For example, disclosing the identity of identified terrorist, while it might cause the terrorists to panic and bring forward their attack, might also alert the public in time and result in prompt arrests. In short, it is our contention that where the classifying authority is unsure he/she should err towards disclosure.[93]

---

[89] At para 93
[90] S 21(1)
[91] 403 US 713 (1971).
[92] Ibid
[93] But see s 14(e) providing that "if there is significant doubt as to whether state information requires protection, the matter must be referred to the relevant Minister for a decision".

Recommendation (2): The Bill should provide a requirement on the part of the classifying officer to give reasons in writing for classifying information or for classifying it in a certain category. Indeed, how else can the officer demonstrate harm to national security if not by giving reasons? The Constitution contemplates under section 33 that all administrative actions that affects or have the potential to affect the right of citizens must be justified by reasons in writing.[94] These administrative actions contemplated in section 33 have been defined broadly to include the implementation of pieces of legislation.[95] Commenting on section 33, the Constitutional Court stated in *President of the Republic of South Africa v South African Rugby Football Union*[96] that:

> The principal function of section 33 is to regulate conduct of the public administration, and, in particular, to ensure that *where action taken by the administration affects or threatens individuals*, the procedures followed comply with the constitutional standards of administrative justice.[97] (Our emphasis)

These constitutional standards of administrative justice include the furnishing of reasons for action taken and ensuring that these actions can be justified by the reasons given.[98] This later requirement is an important ingredient of rule of law. As Chaskalson P, giving judgment for a unanimous court, explained in *Pharmaceutical Manufacturers Association of SA and Another: In re Ex parte President of the Republic of South Africa and Others*[99] case:

> It is a requirement of the rule of law that the exercise of public power by the Executive and other functionaries should not be arbitrary. Decisions must be rationally related to the purpose for which the power was given, otherwise they are in effect arbitrary and inconsistent with this requirement. It follows that in order to pass constitutional scrutiny the exercise of public power by the Executive and other functionaries must, at least, comply with this requirement. If it does not, it falls short of the standards demanded by our Constitution for such action.[100]

This need for classifying authority to furnish reasons for classification has also been recognized in other jurisdictions. For example, in the United State under *Executive Order 13526 of December 29, 2009* that deals with classification of documents, the classification authority is mandatorily required to justify each classification.[101]

Recommendation (3): Clause 13(5) which allows for the classification of entire categories of information even where only minimal amounts of information warrant classification should be deleted as it undermines the intentions and objective of the Bill and makes the bill unconstitutional.

---

[94] Section 33 (c) & (d)
[95] See, for example, *President of the Republic of South Africa v South African Rugby Football Union* at para 142
[96] 2000 (1) SA 1 (CC)
[97] Para 136
[98] See Section 33 (c) & (d) of the Constitution. See also SARFU at Para 45 holding that "the Constitution requires decisions by the President which will have legal effect to be in writing"
[99] 2000 (2) SA 674 (CC)
[100] At para 90.
[101] Section 1.1 of the Executive Order.

As Mokgoro J stated in *Case v Minister of Safety and Security; Curtis v Minister of Safety and Security,* laws that prohibit with the same stroke both constitutionally legitimate and illegitimate activity, are generally regarded as being overbroad and therefore unconstitutional.[102]

5.2. Declassification

The Bill gives the same security organ of state that originally classified information the power to declassify that information.[103] Where a security organ of state has become defunct and there is no successor in function, the Agency would be responsible for handling the classified information and declassifying the same.[104]

Classified information is deemed declassified at the end of a 20-year period.[105] However, this period can be extended if the head of organ of state certify to the satisfaction of the Classification Review Panel that the conditions for classification still apply.[106]

It is our view that the 20 year classification period is too long. An examination of the practice of other countries reveals shorter classification periods. For example,

- The Law on Classified Information of the Former Yugoslav Republic of Macedonia limits State Secrets to 10 years, Highly Confidential information to five years, and Confidential information to three years.
- In Albania, secrets are limited to ten years under the Law on Classified information
- The US Executive Order of 2009 sets a default of ten years unless it can be shown that it needs a longer duration.[107]

Recommendation (1): We recommend that in the interests of promoting access to information, regulated information should be classified for not more than 10 years, followed by renewals of up to five years.

Recommendation (2): The process of automatic declassification of apartheid-era classified documents, as was foreseen in the 2008 version of the Bill, should be restored.

---

[102] 1996 (3) SA 617 (CC) At para 49
[103] Protection of State Information Bill, s 16(1)
[104] Protection of State Information Bill, s 16(4)
[105] Protection of State Information Bill, s 17
[106] Protection of State Information Bill, s 17
[107] See Miklós Harszti, *Access to information by the media in the OSCE region: trends and recommendations. Summary of preliminary results of the survey* Vienna, 30 April 2007

6.0. Chapter 6: Regular Reviews, Request for Access to Classified Information and Status Review

Classified information can be declassified if after a review, carried out at least once every 10 years, the head of organ of state is of the view that they no longer need to be classified.[108]

In addition, declassification may be authorised by a head of relevant organ of state if, after a request, he is convinced that the declassification meets the condition set out in section 14 of the Bill.[109] The head of organ of state is, however, obliged to declassify information, if the information reveals a substantial contravention of, or failure to comply with the law; or an imminent and serious public safety or environmental risk; and if the public interest in the disclosure of the state information clearly outweighs the harm that will arise from the disclosure.[110]

The head of a state organ must decide on a request revealing contravention of, or failure to comply with the law within 14 days and decide on a request revealing risk to public safety or environmental risk within 30 days of the date of receipt of such request.[111] However, where the request reveals none of these listed matters, the request is to be determined within "reasonable time".[112]

It is important to note that the Bill now provide for a public interest override in those instances where the information reveals contravention, or failure to comply with the law; or an imminent and serious public safety or environmental risk. This provision is similar to that of section 46 of Promotion of Access to Information Act (PAIA), which provides that even if there is a ground of refusal applicable to a particular record, the record must still be disclosed if, disclosure "would reveal evidence of … a substantial contravention of, or failure to comply with the law; or … an imminent and serious public safety or environmental risk".[113]

While this is a welcome development in the Bill, it is our view, however, that the public interest override envisaged in both PAIA and the Bill provide too high a threshold. Indeed, the wording of PAIA's public-interest override has been heavily criticised as making the override largely

[108] Protection of State Information Bill, s 18.
[109] Protection of State Information Bill, s 19.
[110] Protection of State Information Bill, s 19(a).
[111] Protection of State Information Bill, s 19(4).
[112] Protection of State Information Bill, s 19(6)
[113] PAIA, s 46

unavailable and arguably unconstitutional.[114] It is our view that this flaw should not have been repeated in the Bill. Instead the drafters should have come up with a simple public interest override that is not burdensome to prove. Words such as "substantial contravention" and "imminent and serious safety" should have been avoided.

In addition, the public interest override envisaged by the Bill is too narrow. We submit that public interest do not only apply to matters of illegality, safety risks or environmental risks. Public interest is a wider concept, which is meant to cover both matters that endanger the public and those that benefit the public. For example, in *Társaság a Szabadságjogokért v. Hungary* ***(****no. 37374/05****),*** the European Court on Human Rights (ECHR) held that research, which would result into the protection of the rights of others, was an exercise in the public interest.[115] In this case, the Applicant required information that would help him in his research on the human rights impact of Hungarian drug-related legislations. The ECHR held that the relevant information should be disclosed to the Applicant on the ground of public interest. In the words of the Court:

> The Court considers that obstacles created in order to hinder access to information of public interest may discourage those working in the media or related fields from pursuing such matters. As a result, they may no longer be able to play their vital role as "public watchdogs" and their ability to provide accurate and reliable information may be adversely affected.[116]

On another note, we submit, that the 10 year review period is unjustifiably too long. An examination of the practice of other countries reveals shorter review periods. For example,

- The Georgian and Estonian State Secrets Act require that each possessor of secrets review the classification yearly and note when it has been declassified.
- In Sweden, the classification is re-evaluated each time the document is accessed.
- Uzbekistan and Turkmenistan require that information is reviewed every five years.[117]

We are also of the view that leaving the determination of requests for information that do not reveal illegality or risk to public safety and environment to "reasonable time" unjustifiably brings uncertainty and makes the provision amenable to abuse. If left unregulated, academicians who depend on time-limited grants for their research would find it difficult to plan their research, especially if the research requires information that needs declassification. We contend that there is no reason why such application should not also be subjected to a *specific* time limit.

---

[114] See Currie & Klaaren *The Promotion of Access to Information Act Commentary* (2002) [7.10]—[7.13].
[115] At para 28 & 34
[116] At para 38
[117] See Miklós Harszti, *Access to information by the media in the OSCE region: trends and recommendations. Summary of preliminary results of the survey* Vienna, 30 April 2007

Furthermore, we are also of the view that Bill must be harmonised with the provisions of the Promotion of Access to Information Act, by requiring a request for access to classified information to be dealt with in terms of the latter Act.

Recommendation (1): To further greater access to information we recommend that reviews of classification be carried out at least once every 5 years.

Recommendation (2): It is recommended that the Bill should provide that once an application for information is made, the relevant authority should not take more than 30 days to arrive at a decision. The time period for requests revealing contravention of, or failure to comply with the law, should remain 14 days.

Recommendation (3): Simplify and broaden the public interest override. Lessons could be learnt from **Ontario's Freedom of Information and Protection of Privacy Act of 1990**, which simply provides at **section 23** that that even if there is a ground of refusal applicable to a particular record, the record must still be disclosed where "a compelling public interest in the disclosure of the record clearly outweighs the purpose of the exemption".[118] The Act lists broad areas of information to which the public interest override is to apply. These include: advice to government, relations with other governments, third party interest, economic and other interests of Ontario, information with respect to closed meetings, public health and safety, personal privacy, and risks to species. We submit that in addition, to information that reveals contravention, or failure to comply with the law; or an imminent and serious public safety or environmental risk, the public interest override in the Bill should also apply to information that reveals risks to public health, defence and security, and international relations. In our view, this broad, open-ended type of provision is more attuned to the requirement of openness and transparency envisaged in the Constitution. In this regard, we can do no better that to quote the words of Justice Stewart, the US Supreme Court Justice in the leading case of *New York Times Company v United States*,[119] which we submit apply with even greater logic in South Africa:

> [Classification] is an awesome responsibility requiring judgment and wisdom of a high order… [A]very first principle of that wisdom would be an insistence upon avoiding secrecy for its own sake. For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion… [T]he hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained[120]

---

[118] S 23
[119] 403 US 713 (1971).
[120] At 729 (Justice Stewart).

Recommendation (4): Harmonise the Bill with the provisions of the Promotion of Access to Information Act, by requiring a request for access to classified information to be dealt with in terms of the latter Act.

7.0. Chapter 7: Classification Review Panel

Chapter 7 creates the Classification Review Panel.[121] The Panel is tasked with, among others, the reviewing and overseeing of status reviews, classifications and declassifications contemplated in the Bill.[122] It is to be composed of 5 personalities competitively recruited by the Joint Standing Committee on Intelligence and appointed by the Minister in charge of Security.[123] In carrying out its function, the Panel "may confirm, vary or set aside any classification decision taken by the head of an organ of state and instruct the head of the organ of state concerned to change the classification status of the classified information, if necessary."[124] A decision of the Panel binds an organ of state subject to any appeal that the organ of state may lodge with a competent High Court.[125] In carrying out its functions, the panel is accountable to the National Assembly, and must report on its activities and the performance of its functions at least once a year.[126]

The inclusion of the Review Panel in the Bill is, in our view, a welcome development. However, this section of the Bill lacks clarity and more detail is needed to ensure that the Panel functions independently of the executive, impartially, is accessible to the public and has binding powers.

Recommendation: The composition and procedures of appointment of the Classification Review Panel should be revised to ensure its independence and impartiality. In this regard, the fact that the Panel's rules are subject to Ministerial concurrence is a concern. Revisions should also clarify the Panel's funding - which it needs to be accountable to the National Assembly for and not the executive – as well as powers and functions. Furthermore, this section should be redrafted to ensure public access to the Panel, and that it has actionable powers.

8.0. Chapter 8: Appeal

[121] Protection of State Information Bill, s 20
[122] Protection of State Information Bill, s 21
[123] Protection of State Information Bill, s 22
[124] Protection of State Information Bill, s 27(1)
[125] Protection of State Information Bill, s 27(3)
[126] Protection of State Information Bill, s 29

If a head of an organ of state denies a request for declassification, the applicant may lodge an appeal with the Minister who is responsible for the particular organ of state within 30 days.[127] The minister must arrive at a decision within 30 days of the date of receipt of such appeal.[128] A person who is not satisfied by the Minister's decision can appeal to the Court.[129] A person can also apply to court directly for urgent relief in cases where classified information reveal contravention, or failure to comply with the law or reveals a risk to public safety and environment. [130]

Evident from this Appeal structure, the Bill does not provide for any kind of an independent arbitrator to consider review and appeal application. The Bill provides that if you want to review a decision to classify, you must take it to the original decision maker and if he refuses appeal to his superior, the Minister. In these circumstances, chances of success are so slim as all the reviews and appeals mechanisms are within the organ of state where the classification happened in the first place. The only outside recourse envisaged by the Bill is the court. However, the cost of accessing courts, including legal fees, filing fees, time, and sometimes distance, make courts inaccessible.

Recommendation: We recommend that appeals against decisions of the heads of organs of state should be made to an independent arbitrator, probably, a retired judge. This would ensure fairness and act as a check against any biasness, real or imagined. The oversight mechanism in New Zealand is relevant in this regard. In terms of **section 28(1) of the Official Information Act 1982**, a person who is aggrieved by a refusal of a request for information under the Act may submit their grievance to the Ombudsman concerned. The Ombudsman may review the documents in question and make a recommendation that the documents be released.[131] All organs of state have a duty to comply with the Ombudsman's recommendation.[132]

9.0. Chapter 9: Transfer of Records to National Archives and Release of Declassified Information to Public

Clause 33 provides for the transfer of classified information to the National Archives. According to the section, the status of all classified information must be reviewed before they are transferred to

[127] Protection of Information Bill, s 31(1) & (2).
[128] Protection of State Information Bill, s 31(3)
[129] Protection of State Information Bill, s 32
[130] Protection of State Information Bill, s 32
[131] Section 30 (1) of the Official Information Act.
[132] Section 32 of the Official Information Act. Section 31(a) of the Act states an Ombudsman may not recommend that the information be made available if the Prime Minister certifies that this would be likely to prejudice national security.

the National Archives.[133] All classified information must be declassified before they are transferred to the National Archives unless the Head of organ of state shows that it still deserves classification in accordance to clause 17.[134]

Under clause 34, classified information that is declassified may be made available to the public in accordance with the Bill, the Promotion of Access to Information Act and any other law.[135] Under clause 34(2) no classified information may be made available to the public until such state information has been declassified or unless ordered by the Court.[136]

Once information has been declassified and released to the public, it may not be reclassified again.[137]

We note that the Bill now makes it clear that with regard to access to *classified* information it will prevail if there is a conflict between its provision and provision of another Act of Parliament that regulates access to classified information.[138] With regard to access to *declassified* information or *valuable* information, the Bill leaves it open. These latter categories of information may be made available to the public in accordance with the Bill, the Promotion of Access to Information Act and any other law.[139] This would mean that, with regard to *declassified* and *valuable* information if an application for access is made under Promotion of Access to Information Act, it shall be considered in accordance with PAIA even if there is a conflict with the Bill. However, with regard to classified information where an application is made under Promotion of Access to Information Act, it shall be considered in accordance with PAIA unless there is a conflict between PAIA and the Bill, in which case the Bill shall prevail.

We contend that the prevalence of the Bill over other laws in matters of access to classified information would only make constitutional sense if its provisions provide easier access to information than the other laws. This, we submit, would only be possible if the issues raised in this paper are addressed.

10.0. Chapter 10: Implementation and Monitoring

[133] Protection of State Information Bill, s 33(1)
[134] Protection of State Information Bill, s 33(2)
[135] Protection of State Information Bill, s 34(1)
[136] Protection of State Information Bill, s 34(2)
[137] Protection of State Information Bill, s 14(i).
[138] Protection of State Information Bill, s 1(4).
[139] Protection of State Information Bill, s 34(1)

Section 35 of the Bill gives the Agency[140] the responsibility of monitoring all organs of state for compliance with the requirements of the law in regard to protection of valuable information and classified information.[141] However, the South African Police Service and the South African National Defence Force are excluded from the ambit of the monitoring responsibility of the Agency.[142]

We do concede that there is need for the implementation of the Bill to be monitored. However, it is our view that if the Bill's objective of decreasing classification and excessive secrecy is to be realised, then the Agency may not be the best actor to be entrusted with the implementation and monitoring thereof. This is because: firstly, intelligence agencies by their very nature are more prone to secrecy than transparency; secondly, member institutions of the Agency being part of the security apparatus should themselves be subjected to monitoring; thirdly, the Agency as envisaged under the Bill is not a singular institution but rather a conglomeration of independent security institutions with divergence functionalities, which would make it difficult for the Agency to discharge its monitoring mandate efficiently and effectively.[143]

We are also not convinced that the South African Police Service and the South African National Defence Force should be excluded from the implementation and monitoring regime given the fact that they are two of the main actors in the maintenance of national security.

Recommendation: In order to encourage independent oversight and efficient implementation, we recommend a constitutional amendment creating an independent Chapter Nine institution with wide-ranging powers headed by a retired judge, to monitor the implementation of the Bill. All organs of state involved in the classification and declassification of state information should be subjected to the monitoring regime. This institution may also be responsible for monitoring the Promotion of Access to Information Act as well.

This recommendation is not novel. For example, in the United State the monitoring of the implementation of classification and declassification law is entrusted to an Information Security

---

[140] **"Agency"** means the State Security Agency contemplated in Schedule 1 to the Public Service Act, 1994 (Proclamation No. 103 of 1994), and includes the National Intelligence Agency, South African Secret Service, Electronic Communications Security (Pty)Ltd (COMSEC), and the South African National Academy for Intelligence. Protection of State Information Bill s. 1

[141] Protection of State Information Bill s. 35

[142] Protection of State Information Bill s 35(b)

[143] Protection of State Information Bill s 2

Oversight Office. **Section 5.2 of the US Executive Order**[144] lists the ISOO's primary functions as including:

> (1) Develop directives for the implementation of this order;
> (2) *Oversee agency actions to ensure compliance with this order and its implementing directives*;
> (3) Review and approve agency implementing regulations prior to their issuance to ensure their consistency with this order and directives issued under section 5.1(a) of this order;
> (4) Have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfil its responsibilities …
> (5) Review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the National Security Advisor;
> (6) Consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order; …
> (7) …
> (8) Report at least annually to the President on the implementation of this order;
> (9) Convene and chair interagency meetings to discuss matters pertaining to the program established by this order.
> (Emphasis added)

11.0. Chapter 11: Offences and Penalties

Section 36 on **"Espionage Offences"** makes it an offence to spy, that is, "to unlawfully communicate, deliver, or make available" classified state information that would "directly or indirectly benefit another state". The penalty is imprisonment for a period ranging from 5 to 25 years depending on whether the information disclosed is confidential, secret, or top secret.

Section 37 on **"Receiving state information unlawfully"** makes it an offence to "unlawfully and intentionally receive state information" which one "knows or ought reasonably to have known would directly or indirectly benefit a foreign state". The penalty is imprisonment for a maximum term of 5, 15 or 25 years depending on whether the information received is confidential, secret, or top secret.

Section 38 on **"Hostile activities"** makes it an offence "to unlawfully communicate, deliver, or make available" classified state information that would "directly or indirectly benefit a non state actor engaged in hostile activity or prejudice the national security of the Republic". The penalty is imprisonment for a maximum term of 5, 15 or 20 years depending on whether the information disclosed is confidential, secret, or top secret.

[144] US Executive Order 13,526 (USEO) issued by President Barack Obama, December 2009.

Section 39 on **"Harbouring or concealing persons"** makes it an offence to harbour or conceal a person who has committed or is about to commit an offence under section 36 or 38. The penalty is imprisonment for a maximum term of ten years.

Section 40 on **"Interception of or interference with classified information"** makes it an offence to access, intercept or interfere with classified information without authority. The penalty is imprisonment for a maximum term of ten years.

Section 41 on **"Registration of intelligence agents and related offences"** makes it an offence to operate in the country or be in the country with the expectation or potential of operating as an intelligence agent of a foreign intelligence or security service without registration. The penalty is imprisonment for a maximum term of five years.

Section 42 on **"Attempt, conspiracy and inducing another person to commit offence"** states that a person who amongst other things "aids, abets… or counsels another person to commit an offence" would be guilty of an offence. The penalty depends on the offence aided and is the same as that meted on the person actually committing the offence.

Section 43 on **"Disclosure of classified information"** imposes a general prohibition on the unlawful disclosure of classified information with a penalty of imprisonment for a maximum term of 5 years.

Section 44 on **"Failure to report possession of classified information"** makes it an offence to fail to report and return classified information unlawfully in ones possession with a penalty of imprisonment for a maximum term of 5 years.

Section 45 on **"Provision of false information to national intelligence structure"** makes it an offence to provide false information to the National Intelligence Structure.[145] The penalty is imprisonment for a maximum term of 5 years.

[145] The "national intelligence structure" is defined to mean: (a) the National Intelligence Coordinating Committee; (b) the intelligence division of the National Defence Force; (c) the intelligence division of the South African Police Service; and (d) the Agency. Protection of State Information Bill, s 1..

Section 46 on **"Destruction or alteration of valuable information"** makes it an offence to destroy of alter valuable information without lawful authorization. The penalty is a fine or imprisonment for a period not exceeding three years.

Section 47 on **"Improper classification of information"** criminalizes the abuse of the classification of information to conceal breaches of the law, administrative errors, embarrassments, and bid riggings. The penalty is imprisonment for a maximum term of 5, 10 or 15 years depending on whether the concealment is classified as confidential, secret or top secret.

Section 48 on **"Failure by head of organ of state or official of organ of state to comply with Act"** makes it an offence for the head or official of an organ of state to "wilfully or in a grossly negligent manner fails to comply with the provisions of this Act." The penalty is imprisonment for a term not exceeding two years.

Section 49 on **"Prohibition of disclosure of state security matter"** makes it an offence to disclose, publish, retain or neglect to take proper care of information which is a state security matter.[146] The penalty is imprisonment for a maximum term of10 years but if it's disclosed to a foreign government the penalty is imprisonment for a maximum term of 15 years.

Any of these acts enumerated as offences would still be offences if committed outside South Africa by South African citizens or any person domiciled in South Africa.[147]

From the outset, we note that the Bill has made a number of positive improvements. **Firstly,** the Bill has removed the minimum sentences in the Offences clause, with the exception of the crime of espionage. The minimum sentences had the effect of aggravating the consequences of accessing information for researchers and would have considerably contributed to muting academic freedom. **Secondly,** the Bill has increased the penalty for improper classification and made it an offence for failure by the head or official of an organ of state to comply with the provisions of the Bill. These provisions would hopefully counter potential abuse of the classification and declassification powers. **Thirdly,** the Bill now provides for whistleblower protection as envisaged under **Protected**

[146] State security matter is defined to include "any matter which is dealt with by the Agency or which relates to the functions of the Agency or to the relationship existing between any person and the Agency". The Protection of State Information Bill, s 1

[147] The Protection of State Information Bill, s 44

Disclosure Act (Act 26 of 2000),[148] section 159 of the **Companies Act (Act 71 of 2008),**[149] and **any other law.**[150] Any other law, could, arguably, include section 29 **the Films and Publications Act of 1996**[151] and section 46 of the **Promotion of Access to Information Act.**[152]

However, despite these welcome improvements, the provisions on offences and penalties still suffer from a number of shortcomings. **Firstly**, it is our view that the penalties for these offences are still severe and disproportionate to the offences in question. Comparable offences in Australia, for example, are subject to imprisonment for a period of two years in relation to the disclosure offence under clause 43 of the Bill, and six months in relation to the continued possession offence under clause 44 of the Bill.[153] **Secondly**, some of the offences put unreasonable onus for compliance on members of the public, which could in turn hamper the long-term realisation of national security. For example, the offence of **providing false information to national intelligence structure** under clause 45 puts the onus of verification of authenticity of information on the supplier of information and not on the state intelligence apparatus. This can discourage the public from sharing information with the intelligence structures unless they are convinced and can defend the authenticity of that information in a court of law if required.

Of particular concern to us, however, is the fact that the Bill fails to provide for public interest defence and public domain defence. The net effect of this lacuna is that if a person, including academics, obtains, holds, releases or publishes information that would serve a greater public interest, like information on grand corruption in government; such a person would be at risk of imprisonment. Similarly, if someone else leaks information and one gets their hand to that information they can be arrested and charged in court because there is no public domain defence - one cannot argue in their defence that the information was or is already in the public domain.

Recommendation: We believe that most of the concerns in the Bill would be addressed if the Bill provides for a public interest defence, crafted in a way that provides for extensive protection and broad applicability, as well as a public domain defence. The public interest defence should apply

---

[148] The Act allows employees to make certain disclosures about their employers which are in the public interest (for example where illegality or criminality has been committed) without suffering reprisals, even, in some circumstances, where disclosure is made to the public at large. See s 9

[149] Section 159 is a provision on protection of whistleblowers.

[150] The Protection of State Information Bill, s 43

[151] For example, s 29(4) of the Films and Publications Act provides that the offence of knowingly distributing a publication which advocates hatred based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm, does not apply to a publication which "amounts to a bona fide discussion, argument or opinion on a matter of public interest".

[152] S 46 obliges classifying authorities to disclose information where public interest in disclosure outweighs the harm in disclosure. Officers who adhere to these provisions would, in our view, escape the penalty of breaching section 43 of the Bill.

[153] Crimes Act of 1914

broadly to where the information reveals incompetence, negligence, criminality, illegality, corruption or hypocrisy on the part of government officials; or where the information reveals risks to the safety, health, security, or defence of the public; or where the public interest in receiving the information outweighs the harm in releasing it. On the other hand, the public domain defence should apply where the impugned information is already in the public domain.

Inclusion of these defences in the Bill would be of particular importance to academicians who mostly rely on information already in the public domain. Researchers would not have to spend their limited research time in confirming the classification status of public information before use. Similarly, the public interest defence would protect researchers who manage to receive banned information on corruption and incompetence in government that has a bearing on the safety, health, defence or security of the public.

While the Bill does recognise the protection of whistleblowers under clause 43, it is our submission that this is not enough. Firstly, the protection of whistle blowing is only guaranteed for the offence of disclosure of classified information. It does not apply to the other offences that equally require protection for disclosure in public interest such as "Prohibition of disclosure of state security matter offence" under clause 49. Secondly, the laws cited under clause 43 only apply to specific categories of protected disclosures such as those made by employees to authorised bodies. They do not apply to disclosures made by the general public, media or researchers. Thirdly, whistleblower protection as envisaged under clause 43 does not apply to persons in possession of classified information already in the public domain.

We submit that the only way to address these shortcomings and make the Bill aligned to the basic constitutional premise of openness and accountability in government is to provide for a public interest defence and a public domain defence.

The introduction of the public interest defence would not be new. It has been introduced in the secrecy laws in other jurisdictions.[154] It has also been recognized at common law where it functions

[154] **Canada**, for example, has introduced a public interest defence, albeit in the context of disclosures by members of the security services. See S 15 of the Security of Information Act, 1985; In **Austria**, the criminal code provides that state secrets are not violated when there is a justified public or private interest. In **Moldova**, Article 7(5) of the Law on Access to Information states that no one can be punished if the public interest in knowing the information is larger than the damage that can result from its dissemination; In **Georgia**, the Law on Freedom of Speech and Expression says that those who disclose state secrets are not liable 'if the purpose of disclosure of a secret was protection of the lawful interests of the society, and if the protected good exceed the caused damage.' See Law Reform Commission Working Paper 49 quoted in *Backgrounder No.12 – Security Information Act,* April 2004. Canadian Security Intelligence Service. Available online: http://www.csis-scra.gc.ca/bckgrndrs/bckgrndr12-eng.asp (last accessed 21 June 2011)

as a defence to an infringement of privacy.[155] The Constitutional Court has also recognized the importance of public interest in the context of security cases. In *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services* it said:

> On the other hand, the circumstances in which an intelligence agency came to improperly and unlawfully infringe upon the privacy of an innocent citizen are not merely matters of public curiosity. They would be issues of immense public interest. The degree of public interest is an important factor to be put into the balance and would, in my view, not be of insignificant weight if the interest is one that must be fulfilled…[156]
>
> The public importance of and interest in these events can neither be gainsaid nor over-emphasised. A member of the public was unlawfully and improperly harassed and he and his family suffered an egregious and inexcusable invasion of privacy. All this consequent upon secret government action. The public is entitled to know all except that which cannot be revealed on account of important national security considerations. I would put the strong public interest to know as well as the extent to which the material is already in the public domain on the one side of the scale and the appropriate weight to be attached to the government objection on the other side of the scale in order to determine where the balance falls in the interests of justice enquiry. …[157]
>
> The starting point of the enquiry into whether the document should be released is that it was of great public importance and justified considerable public interest.[158]

Similarly, providing for public domain defence would align the Bill with the recognized principle of confidentiality, which states that it is futile to protect information that has lost its secrecy. This principle has been recognized in a number of legislations and by a number of courts. For example, section 37(2) of the Promotion of Access to Information Act provides that disclosure of confidential information "already publicly available" may not be refused. The South African Courts have also recognized the principle in the area of commercial confidentiality,[159] and law of privacy.[160] The Constitutional Court has specifically stated that "[i]f the information is already lawfully in the public domain there can be no reason for its non-disclosure."[161] Other jurisdictions have also applied the concept in the context of national security restrictions.[162]

It is also worth mentioning that the Ministry of Intelligence had indicated in the *Explanatory Note on the 2008 Bill* that "the Minister has no objection to the inclusion of a public interest

---

[155] For example, in the case of *Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another* 1993 (2) SA 451 (A), the Appellate Division held as follows:

> It might well be that, if in the case of information obtained by means of an unlawful intrusion the nature of the information were such that there were overriding grounds in favour of the public being informed thereof, the Court would conclude that publication of the information should be permitted, despite its source or the manner in which it was obtained.

At para 463. See also *MEC for Health, Mpumulanga v M-Net* 2002 (6) SA 714 (T) at para 2

[156] At para 88.

[157] At para 103.

[158] At para 121. Although Yacoob J's decision was a minority decision, his analysis illustrates for present purposes the importance of ensuring that a public interest defence to the disclosure of classified information should be crafted, lest the media is chilled from disclosing matters of immense public significance for fear of the severe penalties that may ensue.

[159] See e.g. Valunet Solutions Inc t/a Dinkum USA v eTel Communications Solutions (Pty) Ltd 2005 (3) SA 494 (W) at para 17.

[160] See generally J Neethling, JM Potgieter & PJ Visser *Neethling's Law of Personality* (2nd edn, 2003).

[161] See *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services* at para 91. See also para 55, 62 & 103

[162] See, for example, the English case of *Attorney-General v Guardian Newspapers*(No 2) at 642; and the European Court of Human Rights case of *Verenigung Weekblad Bluf V Netherlands*(1995) 20 EHRR 189.

exemption".[163] The drafters of the revised version of the Bill have, however, contend: **first**, that its inclusion would create legal uncertainty;[164] **second**, that in any case the defence already exist under the common law;[165] and **third**, that the public interest defence clause will make the bill useless, as it will mean that classified info will already be in the public domain when the court hears the matter.[166]

It is our view, however, that these contentions should not hold sway. **Firstly**, as demonstrated above, the South African courts have a rich experience in applying the public interest defence and would definitely have no difficulty in developing jurisprudence to address it in the context of the Bill. In any case the enjoyment of Bill of Rights, specifically the right to access to information and freedom of expression should not be sacrificed at the altar of a desire to create legal certainty. **Secondly**, there is no general common law defences of "public interest" that apply to all offences created in statutes. **Thirdly**, the argument that classified info will already be in public domain when the defence is raised in court is far-fetched since nobody would risk imprisonment by disclosing information that does not meet the requirement of public interest. The penalty for not meeting the standard of public interest in itself is a check against abuse of the defence. In any case, the government is precluded from viewing its citizens with distrust and enmity and should not legislate on the basis of fear. As Sach J said in *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services:*[167]

> An open and democratic society does not view its citizens as enemies. Nor does it see its basic security as being derived from the power of the state to repress those it regards as opponents.[168]

12.0. Chapter 12: Protection of information in courts

Clause 52 of the Bill deals with protection of State information before courts. In a nutshell it provides that information before a court may not be disclosed to unauthorised persons unless ordered by the court.[169] Where the court is of the view that whole or part of the information should remain confidential, then it must adopt a procedure that would protect that information from disclosure during the course of legal proceedings including the holding of proceedings *in camera*.[170]

---

[163] At para 120.7.
[164] This statement was made in the Presentation to the Ad Hoc Committee on the Bill dated 7 May 2010. A copy of the presentation is available at www.pmg.org.za (Accessed on 2 June 2010).
[165] This suggestion was made during the briefing of the Ad Hoc Committee by the Minister of State Security on 7 May 2010. A minute of the briefing is available at www.pmg.org.za (Accessed on 2 June 2010).
[166] This argument was made by State Security Minister Siyabonga Cwele during debate on the Bill in Parliament.
[167] 2008 (4) SA 31 (CC)
[168] At para 155.
[169] Clause 52(2)
[170] Clause 52(3)

This provision, simply put, tries to limit the right to open justice in the context of classified information.[171] The importance of this right has been recognized by the Constitutional Court. In *Shinga v The State,*[172] Yacoob J explained the constitutional interest in open justice in the following terms:

> Seeing justice done in court enhances public confidence in the criminal-justice process and assists victims, the accused and the broader community to accept the legitimacy of that process. Open courtrooms foster judicial excellence, thus rendering courts accountable and legitimate. Were criminal appeals to be dealt with behind closed doors, faith in the criminal justice system may be lost. No democratic society can risk losing that faith. It is for this reason that the principle of open justice is an important principle in a democracy.[173]

Earlier on in *S v Mamabolo*[174] the Constitutional Court had observed:

> Since time immemorial and in many divergent cultures it has been accepted that the business of adjudication concerns not only the immediate litigants but is a matter of public concern which, for its credibility, is done in the open where all can see. Of course this openness seeks to ensure that the citizenry know what is happening, such knowledge in turn being a means towards the next objective: so that the people can discuss, endorse, criticise, applaud or castigate the conduct of their courts and, ultimately such free and frank debate about judicial proceedings serve more than one vital public purpose. Self evidently such informed and vocal public scrutiny promotes impartiality, accessibility and effectiveness, three of the more important aspirational attributes prescribed for the judiciary by the Constitution ….
>
> However, such vocal public scrutiny performs another important constitutional function. It constitutes a democratic check on the judiciary. The judiciary exercises public power and it is right that there be an appropriate check on such power.[175]

Of course, this right is not absolute and may be limited in the interest of justice.[176] For example, the right may be limited when fair trial rights or dignity or rights of a child or rights of other vulnerable groups are implicated.[177] However, it is our contention that the manner in which the right has been limited in the Bill is indefensible. We base our contention on the criteria set out by the

---

[171] The right to open justice has been identified to flow from a number of rights in the Bill of Rights including right to fair trial, right to access to information and freedom of expression.

[172] *Shinga v The State and Another (Society of Advocates, Pietermaritzburg Bar as* Amicus Curiae*); O'Connell and Others v The State* [2007] ZACC 3; 2007 (5) BCLR 474 (CC); 2007 (4) SA 611 (CC).

[173] At para 26

[174] At paras 28-9.

[175] For equivalent foreign law, see *Richmond Newspapers Inc v Virginia* 448 US 555 (1980) at 570-2; *Edmonton Journal v Attorney General for Alberta*, *Attorney General of Canada and Attorney General of Ontario* [1989] 2 SCR 1326, 64 DLR (4th) 577; Named Person v Vancouver Sun 2007 SCC 43.

[176] See, for example, *Richmond Newspapers Inc v Virginia* 448 US 555 (1980) at 570-2; *Edmonton Journal v Attorney General for Alberta, Attorney General of Canada and Attorney General of Ontario* [1989] 2 SCR 1326, 64 DLR (4th) 577; *Named Person v Vancouver Sun* 2007 SCC 43.

[177] Section 153(1) of the Criminal Procedure Act 51 of 1977 provides that:

> If it appears to any court that it would, in any criminal proceedings pending before that court, be in the interests of the security of the State or of good order or of public morals or of the administration of justice that such proceedings be held behind closed doors, it may direct that the public or any class thereof shall not be present at such proceedings or any part thereof.

Similarly, section 5(2) of the Magistrates' Courts Act 32 of 1944 states that:

> The court may in any case, in the interests of good order or public morals, direct that a civil trial shall be held with closed doors, or that (with such exceptions as the court may direct) minors or the public generally shall not be permitted to be present thereat.

In terms of section 56 of the Children's Act 38 of 2005, proceedings of a children's court are closed and may be attended only by certain persons specifically mentioned in the section.

Constitutional Court for balancing the national security interests and the right to open justice. In *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services* the Court stated:

> In each case, the Court will have to weigh the competing rights or interests carefully with the view to ensuring that the limitation that it places on open justice is properly tailored and proportioned to the end it seeks to attain. In the end, the contours of our constitutional rights are shaped by the justifiable limitation that the context presents and the law permits …[178]
>
> it is so that a party that contends for a restriction of a right protected in the Bill of Rights must place before the Court material which justifies the limitations sought … at the end of the day, a Court is obliged to have regard to all factual matter and factors before it in order to decide whether the limitation on the right to open courtrooms passes constitutional muster....[179]
>
> [T]he starting point is that court proceedings and so too court records must be open to the public.[180]

Drawing from this direction of the Court, it is our view that clause 52 undermines the principle of open justice in a number of respects. First, it envisages the starting point to be that classified information before a court may not be disclosed unless a court orders disclosure.[181] This is inconsistent with the jurisprudence adopted with regard to limitation of constitutional rights. As the Constitutional Court stated in *Independent Newspapers (Pty) Ltd v Minister for Intelligence Services,* "[T]he starting point is that court proceedings and so too court records must be open to the public."[182]

Secondly, the mandatory tone of s 52(5) requiring that hearings on disclosure of documents must be held *in camera* and its dictate that submissions made by the classifying authority may not be publicly disclosed, not only hamper the discretion of courts but also places unjustifiable constraints on the right to open justice.[183] As the Constitutional Court noted in *Independent Newspapers (Pty) Ltd*, the general principle, even in the case of classified information before the Court, is that hearings take place in the open and that documents relevant to that hearing be made accessible to members of the public.[184] It follows that non-disclosure should be the exception and not the rule.

---

[178] At paras 45-6.

[179] At para 45.

[180] At para 54.

[181] See s 52(2) providing that:

> Classified information that is filed in the manner contemplated in subsection (1) may not be disclosed to persons not authorised to receive such information unless a court, in the interests of justice, and upon considering issues of national security, orders full or limited disclosure, with or without conditions.

[182] At para 54.

[183] See s 52 (4) A court may not order the disclosure of classified information without taking reasonable steps to obtain the written or oral submissions of the classification authority that made the classifications in question or alternatively to obtain the submissions of the Director-General of the Agency; and

(5) If it appears to a court that it would, in any hearing held in terms of this section be in the interest of national security or in the interest of justice that such hearing be held *in camera* or that the submission referred to in subsection (4) be not publicly disclosed, the court may direct that the hearing must be held *in camera* and that any person not authorised to receive such classified information may not be present at such hearing.

[184] At para 54.

Thirdly, section 52(6), which gives a blanket prohibition to the disclosure of classified information to interested parties, is also out of tune with the criteria for balancing national security and open justice.[185] As Moseneke DCJ stated in *Independent Newspapers (Pty) Ltd*

> I do not mean to lay down an inflexible rule. There will be instances where a party will point to what appears to be a lack of authority or to an improper exercise of authority or to some other unjustifiable conduct on the part of a public official claiming confidentiality of information. In that event, it may well be in the interests of justice to permit the party concerned and her or his legal representatives, subject to appropriate conditions, to gain access to the sealed part of the record or information for purposes of posing an informed challenge to the confidentiality claim of the public official concerned[186]

Recommendation: The entire provision of clause 52 of the Bill should be amended to reflect the principle of open justice in that all documents placed before the court, whether classified or not, should be accessible to the public, unless a court, in the interest of justice, orders otherwise.

13.0. Chapter 13: General Provisions

Chapter 13 addresses itself to miscellaneous provisions on reporting structure;[187] areas for regulation;[188] transitional provisions;[189] repeal of laws;[190] short title of the Act and the commencement date.[191] We have not identified any areas of potential infringement to academic freedom under this chapter. We are, however, a live to the fact that, apart from the Protection of Information Act of 1982, which the Bill seeks to repeal, there are other pieces of legislation dealing with confidentiality and classification of state information, which if left untouched may create confusion in the classification regime. Some of these legislations have been identified to be in conflict with the Bill and in some instances more restrictive to access to information. These legislations include: Defence Act 42 of 2002;[192] Intelligence Services Act 65 of 2002;[193] and The National Supplies Procurement Act 89 of 1970.[194] We **recommend** that the Bill should repeal *all* inconsistent provisions in the existing statutes in order to align them with the new classification regime that it proposes.

---

[185] S 52 (6): A court may, if it considers it appropriate, seek the written or oral submissions of interested parties, persons and organisations but may not disclose the actual classified information to such persons or parties prior to its order to disclose the information in terms of subsection (1).
[186] At para 32, our emphasis
[187] S 53
[188] S 54
[189] S 55
[190] S 56
[191] S 57
[192] See, for example s 104.
[193] See, for example s 10.
[194] Section 8A.

We are also aware that the Minister has been given broad discretion under section 54 in coming up with regulations and national information security standards and procedure. As a check on potential abuse of discretion, we recommend that a proviso requiring that the Minister's prescriptions must not be inconsistent with the Bill should be inserted. The Minister should also be made obliged to give proper consideration to all comments received under section 54(5). This latter proposal is in line with section 4(3) of the Promotion of Administrative Justice Act 3 of 2000 which provides:

> If an administrator decides to follow a notice and comment procedure, the administrator must—
> *(a)* take appropriate steps to communicate the administrative action to those likely to be materially and adversely affected by it and call for comments from them;
> (b) consider any comments received;
> (c) decide whether or not to take the administrative action, with or without changes; and
> (d) comply with the procedures to be followed in connection with notice and comment procedures, as prescribed.

PART B

In part A the interests of academic researchers in the free flow of information were highlighted in relation to specific concerns with the Bill. In this part of the submission, research projects that could be affected by the Bill are considered.

Dr Laurie Nathan – research fellow, University of Pretoria (UP) and University of Cape Town (UCT)

Nathan is a research fellow at UP and UCT and specialises in research about international relations, especially state security in the SADC region. Where Nathan's research focuses on the security of South Africa his research falls directly within the ambit of the current definitions of the Bill.

In a 2006 paper,[195] Nathan refers to the 'military and political disaster' of the 1998 invasion of Lesotho by South Africa and Botswana. Some information about this invasion is in the public domain, but it is possible that other information exists which could still remain classified for another 7 years under the lengthy 20 year classification period described by the Bill. The lengthy time restrictions and onerous access provisions may discourage researchers from pursuing research in this regard.

While exploring the domestic intelligence mandate and its history in South Africa, Nathan (2009) explains that in the years following the end of apartheid the National Intelligence Agency interpreted its mandate "narrowly, concentrating on terrorism, sabotage, subversion and organized crime". Following the appointment of Joe Nhlanhla as the first Minister of the newly formed Intelligence Services ministry in 1999, the NIA's mandated was greatly, and perhaps dangerously, expanded. Nathan explains that the expanded interpretation of its mandate was contained in a classified operational directive to the NIA, and "entailed a staggeringly broad approach to security that encompassed political, social, economic and environmental issues and was not limited to threats but also included the identification of opportunities. This directive presented five categories under the heading "Broad Areas of Interest and Focus", namely: political intelligence, economic intelligence, organized crime and corruption and special events (Nathan 2009: 163). Following an "intelligence crisis" in 2005/6, the NIA made efforts to move away from political intelligence, and opted to rephrase this part of its mandate to that of "Social Stability Intelligence" (2009: 164). Nathan explains:

> The aim was to meet the human security challenges of South Africa as a developmental state by focusing on two components, namely threats and risks to political stability and threats and risks to social stability. In the view of the [Ministerial Review Commission of Intelligence], this sweeping

[195] Nathan, L. 2006. "Domestic Instability and Security Communities" in *European Journal of International Relations* (12: 275). Published by: Sage publications. http://ejt.sagepub.com/content/12/2/275 (21 July 2011)

> reformulation would do nothing to ease the difficulty of ascertaining the NIA's mandate with any precision. (Nathan 2009: 164)

This broad mandate of the NIA is not only crippling for the agency itself, in that it impedes effective management of intelligence services and leads to a lack of focus, but is also dangerous in light of the powers of information classification awarded to the NIA by the POSI Bill. In fact, the NIA's "thematic scope is so wide that it embraces the focus of virtually every state department," Nathan explains (2009: 164). As operational policies of the NIA (which has since been incorporated into the State Security Agency) will probably remain confidential once the Bill is passed into law, such research will become difficult, if not impossible, to undertake.

Engineering project – UP

The University of Pretoria and their engineering department is currently involved in research that may be in violation of the Protection of Information Bill. Very briefly, this research project entails research of the FM spectrum, and as a result UP staffers have occasionally crossed a 'confidential' band of radio. Naidoo, the research director at UP, said that while this research may have possible repercussions for communications in South Africa, he was concerned as to what would happen to this research project and its researchers were the Bill implemented. He expressed concern that, not only would the research project be effectively shut down, but the researchers may also be penalised for accessing the confidential FM bands in the first place.

Naidoo was quite vague with regards to this project, assumingly because of its ongoing nature. He added that he felt that government itself does not have adequate respect for issues of confidentiality. Naidoo explained this by saying that, as a former government staffer himself, he is aware that information was often leaked, or even purposely publicly distributed, when it should have remained confidential. Naidoo blamed this on a lack of training in terms of this kind of communication in government departments. He added that government should be better prepared to protect or limit access to (certain) kinds of information, instead of penalising academics and other members of society once they access a piece of classified information.

Christopher McMichael – Phd student, Rhodes University[196]

Christopher McMichael is a PhD candidate in the politics department of Rhodes University. His research investigates the ways in which the international governing body of football, FIFA, used the

[196] Duncan, J. 2011. "The Prevention of Scholarship Bill". Published by Sacsis. http://www.sacsis.org.za/site/article/686.1 (accessed: 18 July 2011).

security arrangements for the 2010 World Cup to cannibalise public funds to the benefit of the Association and its sponsors.

South Africa had to develop complex security plans and invest in state of the art security equipment to meet FIFA requirements, at huge expense to the taxpayer. Policing culture also became more militaristic in the preparations for the mega-event, resulting in the introduction of the military ranking system in the South African Police Services (SAPS) and the 'shoot to kill injunction.'

In his research, McMichael asks whether the fact that no major security incidents took place during the event be attributed to the 'success' of the security measures, or whether 'mega-event security has become increasingly decoupled both from proportionality and perhaps even reality?'

South Africa is now living with the legacy of having hosted a successful World Cup. But the downsides have become increasingly apparent, with the Nelson Mandela Bay facing a massive debt crisis, and Johannesburg commuters being faced with the prospect of having to pay for the upgrading of highways through toll fees. The militarised policing style remains, and has led to several civilians being shot dead needlessly. McMichael's research is important as it should make South Africans think about the costs of hosting mega events relative to the benefits. In the course of undertaking his research, McMichael attempted to interview the police, but without success. As a result, he has to rely on documentation. He managed to access the Bid Book before the document was embargoed, which outlined, amongst other things, an assessment of the government's capacity to meet the expected standard required of FIFA.

An SAPS office in one host city refused an interview, but instead sent him a copy of their final security plan, in spite of the fact that the document was marked 'confidential'. This document helped McMichael show how the safety and security measures were implicitly designed to benefit FIFA, while ostensibly being about guaranteeing public safety. For instance, it showed how airspace restrictions were developed to prevent both '9/11' style attacks and skywriting by non-affiliated brands, thereby revealing the extent to which 'national security' converged with corporate interests.

If the Bill were passed into law, McMichael would be guilty of an offence for possession of a classified document, and in the absence of a public interests defence, he could be prosecuted and jailed. This research currently being undertaken by McMichael will fall squarely within the ambit of

the Bill, and even if he is not penalised for his acquisition of the ‘confidential’ document, his research may be declared confidential due to its nature.

14.0. Conclusion

This paper has attempted to analyse the provisions of the proposed Protection of State Information Bill and to demonstrate how its enactment might affect the exercise of the right to academic freedom. The Bill, as shown, provides for the protection of state information that requires protection. It aims to balance the presumption of secrecy with a presumption of openness. To realize this aim, the Bill relies on the well established assumption in Administrative law that decision makers or public officials will do their job and have no incentive to hide corruption, malpractices or illegalities.[197] As such the Bill gives heads of organs of state security and their nominees' power to determine which information warrants classification and which one does not. Yet, it is this unqualified trust in the competence and incorruptibility of the decision makers that is proving to be the Bill's Achilles' heel. The problem, as demonstrated, is that some critical words and phrases have been left loosely defined, so much so that even a well meaning officer would have difficulty in knowing how to make decisions about them.

As the Constitutional Court has warned:

> It is an important principle of the rule of law that rules be stated in a clear and accessible manner. It is because of this principle that section 36 [of the Constitution] requires that limitations of rights may be justifiable only if they are authorised by law of general application. Moreover, if broad discretionary powers contain no express constraints, those who are affected by the exercise of the broad discretionary powers will not know what is relevant to the exercise of those powers or in what circumstances they are entitled to seek relief from an adverse decision.[198]

It is imperative therefore that the Bill clearly defines its scope of operation. Legislation regulating access to information held by state security bodies is necessary. However, the regulation must be in line with the Constitution and the rights protected thereby. Academic freedom, an important aspect of freedom of expression exists, is constitutionally protected. Academic research on issues of national security is important since it ensures accountability, engenders discussion and involves citizens in the affairs that affect their well-being.

---

[197] For a discussion of this principle *see Pharmaceutical Manufacturers Association of South Africa: In Re: Ex parte Application of the President of the Republic of South Africa* 2000 (2) SA 674 (CC)

[198] *Dawood v Minister of Home Affairs* 2000 (3) SA 936 (CC), at para 47

We conclude where we should have started, by placing a caveat that the preceding discussion on the provisions of the bill is not final. It is an attempt to detain a moving target and study its intended direction. Such a study, we submit, cannot be detailed or specific. As a consequence, this paper has only given a general overview of the various chapters in an effort to direct the effort towards a realisation of a constitutionally compliant Bill. We believe that if the issues raised in this paper are addressed then the Bill would make the necessary step towards respecting the right to academic freedom. As noted by the Constitutional Court in *Brummer v Minister for Social Development and Others*[199] "… access to information is crucial to the right to freedom of expression which includes freedom of the press and other media and freedom to receive or impart information or ideas".[200]

We submit that if the issues raised in this paper are not addressed, then the enjoyment of right to academic freedom would suffer irreparably. The reasons for this are not hard to imagine. Some of them include:

1. Academicians whose research depends on classified information would not be able to plan their research work since the period for determination of requests for information has been left to the nebulous "reasonable time." The implication of this problem is especially severe for researchers who depend on time-limited grants.
2. Researchers will now have to, in addition to researching for relevant information, confirm with over 100 classification authorities whether the information they gleaned from public sources are classified or not. Otherwise, they risk being slapped with an imprisonment term ranging from 5 years to 25 years for obtaining, holding, releasing or publishing classified information. Where is the time and resources for all these confirmations, we ask?
3. Publication of research in relation to the security cluster is put into jeopardy. Since the application, review and appeal for access to information in this area has been restricted to those officials and line ministers who classified the information in the first place, it would now be nigh impossible to get information especially on controversial projects that require review. The situation is not made easier by the fact that the Bill does not protect researchers who somehow manage to get the information from employees working in these areas. While the whistleblower is protected from prosecution for disclosure, the researcher is not and can face imprisonment for a term ranging from 5 years to 25 years depending on the type of information received/published.
4. Research into court proceedings and critique of court judgments is made impossible especially in those cases where evidence and documents relied on by the Courts in reaching their conclusions are classified. This is because courts are now precluded from enclosing those

[199] CCT 25/09) [2009] ZACC 21; 2009 (6) SA 323 (CC) ; 2009 (11) BCLR 1075 (CC) (13 August 2009)
[200] At para 63 (footnotes omitted). Academic freedom is part and parcel of the right to freedom of expression.

evidences in their judgments. A researcher who wishes to critique the conclusions of the judges would now have to apply to the relevant Court for access to these classified evidences. The attendant cost and time makes this area a no-go zone for many, if not most, researchers.

5. Researchers and students from foreign countries have now been exposed to unreasonable suspicion and intimidation by section 41 of the Bill, which makes it an offence to be unregistered intelligence agent if you have the *potential* or *expectation* of being a foreign intelligent agent. How does the government determine that a person is a potential agent or is expecting to be an agent if not by constant surveillance or introduction of new conditions for visa applications? If uncircumscribed, this provision could hamper international academic exchange and collaboration among scholars, and contribute to a drop in foreign-student/scholar applications to South African colleges and universities.

South Africa has a sorry history of abuse of the state security apparatuses, and Universities have a key role to play to ensure that such abuses are not repeated. Researchers need access to documents that expose the inner workings of the security cluster, and its interface with society. If the Bill remains as is, then such research will be exceedingly difficult, if not, impossible, as the security apparatus will remain largely off limits. This culture of secrecy creates conditions where a securitisation of the state could take place unchecked, with potentially negative implication for South Africa and the region as a whole.

Research that is of considerable public importance - such as research into the restructuring and 're-militarisation' of the police and its relationship to growing police violence, and research into the transformation of the military – will be extremely difficult to undertake. Researchers will also find it exceedingly difficult to enquire into whether the intelligence structures are being used to ensure civilian safety rather than the harassment of political opposition. Any research that is in the public interest, but that is based on leaked classified information, could be criminalised and the researcher could be arrested for failing to report possession of classified information. The Bill does penalise those who classify information for improper purposes, such as to conceal corruption or prevent embarrassment. However, there are many documents that may be classified for what the Bill considers to be 'proper reasons' that researchers will be unable to access, given the overbroad definition of what constitutes national security.[201]

[201] Rhodes University, Information Bill: changes welcome, more needed, statement issued on behalf of Senate and Council, 14 July 2011.

This paper has identified the areas of concern and given specific recommendations in each of the identified areas of concern which it hopes would help reduce the negative impact of the Bill on academic freedom. While the Bill is a considerable improvement on the version tabled initially, aspects of the Bill still favour secrecy above openness and transparency in the organs of state security in a manner that threatens academic freedom. It will probably lead to information plugs developing in the system, obstructing research and disillusioning researchers. Future researchers may shy away from undertaking research on the security cluster owing to the difficulties and even risks involved. The Bill may also lead to unwarranted interference from the state in academic activity.

As a result, it is important for universities to audit the implications of the Bill for their work by identifying projects that may be affected by the Bill, and develop positions that could then be used to lobby the National Council of Provinces to make changes to the Bill that take academic freedom, and the related freedoms of expression and access to information into account.

End