Submission to the National Council of Provinces
The Protection of State Information Bill
February 2012

Submitted by the Helen Suzman Foundation
1. Introduction

The passage of this Bill has been poorly managed. The result has been the creation of an extremely tense environment. The adverse effect of this environment on the policy processes is notable for the very reason that the debates around this Bill have become polarised.

There is a growing conviction that the Bill has been driven by narrow political interests instead of considering the broader societal interests of South Africa as a country, particularly when the issues at hand have the potential to seriously alter relations between the state, its different levels of government and citizens. In addition, the focus on a public interest defence, vital as this is, has meant that many other serious issues pertaining to this Bill have been overlooked.

In order to provide clarity, and in line with its mandate to promote constitutional democracy by informed and reasoned debate around policy issues as they relate to South Africa and its Constitution, the Helen Suzman Foundation (hereafter “the Foundation”) makes this submission on the Protection of State Information Bill.

This submission is not made in a vacuum. The Foundation has closely monitored the passage of the Bill and has, on occasion, made its concerns known\(^1\). Due to the antagonism between the advocates of this Bill and those who have raised concerns over certain features of the Bill, it seems fair to note that the advocates of this Bill have been less than willing to take the legitimate concerns and objections raised by civil society formations and opposition groups onboard. Only when opposition has been raised to fever pitch levels has any compromise been forthcoming. This indicates a worrying trend within policy debates in South Africa which, if allowed to continue, will only result in poorer policy choices being taken, and leaving South Africans worse off\(^2\).

---


The first draft of the 2010 Bill galvanised civil society formations and opposition groups which view the Bill as an attempt by the security cluster to draw a veil of secrecy over the operations of state. The comments of the Security Ministry have done little to dissuade anyone from holding that view. This battle culminated with the ANC majority in Parliament, under a three line whip and notwithstanding internal opposition and dissent, passing the Bill in the National Assembly on 22 November 2011.

This submission begins its review of the Bill via a comparative and international overview, and sets out to contextualise the environment in which many democratic states have pushed through wide reaching National Security type legislation. It is important to read the Protection of State Information Bill against this backdrop because of the Bill’s reliance on National Security concerns as a defence for the Government to enact such legislation. The sections that follow will explore the merits of key parts of this Bill – relying on the Constitution, as providing South Africa’s legal framework, for guidance in determining the value of this Bill as it is currently drafted. The premise from which this document begins its review is a presumption in favour of the constitutional imperative for freedom of expression.

*Protection of State Information, National Security concerns, and Secrecy* are all terms which have made a forceful comeback into the language of the democratic state in recent times. Across the globe there has been a growing tension between advocates of access to information and those who push for greater secrecy as a National Security imperative. Arguably, September 11, 2001 was the catalyst for many governments to push through legislation aimed at ‘protecting national security’. It is the Foundation’s concern that legislation of this nature has the tendency to be excessive and may lead to severe limitations on civil and political rights enjoyed by citizens of democratic states.

The Patriot Act (2001) in the United States, for example, has curtailed a number of civil liberties and has increased the power of the government to monitor its own people through all sorts of surveillance operations without securing warrants to do so. While the government officials responsible for this legislation have argued they are necessary, given the constantly evolving threats that exist in this modern era, many of these pieces of legislation were rushed through by politicians in an environment of fear and confusion. The Patriot Act, for example, was passed a mere 6 weeks after the attacks of 9/11.

The Patriot Act, along with the Homeland Security Act (2002), have completely reorganised the relationship between an individual’s privacy and the ability of the state to infringe on that privacy in the United States. In a classic case of national security legislation overstepping its bounds a number of court cases were filed against the government for illegal wire tapping of individuals. On 31 March 2010 a federal judge ruled that the National Security Agency’s programme of surveillance without warrants was illegal\(^3\).

The UK government has also responded with a wealth of legislation (the Anti-terrorism, Crime and Security Act 2001, and the Terrorism Act 2006) that has significantly altered the criminal law as it relates to police investigations, police powers and prosecutions in terrorist

---

offences. Many new offences have been created, police powers have been expanded, and the relationship between the state and the individual appears to have been fundamentally altered.

Very little analysis of the implications to citizen’s rights was carried out. Legislation of this type can be extremely dangerous if it is not drafted carefully and in a transparent and accountable manner. Due to its very nature legislation that has as its primary driver National Security imperatives, places immense power in the hands of those who implement it, which is why it is important for all actors to be informed of the nature of the legislation and aware of the consequences for individual freedoms. The same may be said of legislation which seeks to limit the free flow of information between the citizenry and their government.

National Security is a contested term as it can include a number of variables in differing shades of significance, but taken as a whole can have significant consequences on the relationship between the government and the citizenry of any country.

A leading commentator on national security has argued that the reason national security remains a “weakly conceptualised, ambiguously defined, but politically powerful concept” is that “for the practitioners of state policy, compelling reasons exist for maintaining its symbolic ambiguity... An undefined notion of national security offers scope for power maximising strategies to political and military elites, because of the considerable leverage over domestic affairs which can be obtained by invoking it”\(^4\). It is a term which its advocates will continually fall back on in order to maintain a veil of secrecy over their actions.

It is for this very reason that National Security concerns must be clearly stated and narrowly defined so as to complement any constitutional imperatives which favour open and transparent government. In any constitutional democracy the rights of citizens should supersede the use of National Security legislation which, due to its often very broad application, must remain the exception to the rule.

3. The Protection of State Information Bill – The South African Process

The Protection of State Information Bill first made an appearance in 2008 under the then Minister of Intelligence, Ronnie Kasrils. Mr Kasrils has maintained that he sought to create legislation that would protect state secrets but also uphold the constitutional principal of transparent governance.

The 2008 version of the Bill included a provision that would allow whistleblowers to leak information that was in the public interest without fear of reprisal. When the Bill made its reappearance it looked nothing like the 2008 version, and has been described as draconian and excessive in a number of media reports and civil society publications.

The Ministerial Review Commission on Intelligence issued its final Report to Minister Kasrils on September 23 2008. It had the following considerations to bear in mind:

“In order to fulfill their vital functions, intelligence services throughout the world are able to operate secretly and have special powers to acquire confidential information through surveillance, infiltration of organisations, interception of communication and other methods that infringe the rights to privacy and dignity. Politicians and intelligence officers can abuse these powers to infringe rights without good cause, interfere in lawful politics and favour or prejudice a political party or leader, thereby subverting democracy. They can intimidate the government’s opponents, create a climate of fear and manipulate intelligence in order to influence state decision-making and public opinion. Given these dangers, democratic societies are confronted by the challenge of constructing rules, controls and other safeguards that prevent misconduct by the intelligence services without restricting the services to such an extent that they are unable to fulfill their duties. In short, the challenge is

---


6 Ibid

to ensure that the intelligence agencies pursue a legitimate mandate in a legitimate manner\textsuperscript{8}.

The Report makes a clear case for treading cautiously around legislation that seeks to draw a veil of secrecy over the operations of the state, based on past experiences, and the ability of those in power to subvert secrecy legislation for their own narrow interests, which may run counter to the constitutional rights of citizens. While acknowledging that States commonly have legislation in place to protect certain types of information from unlawful disclosure, the broad use of National Security imperatives must be kept to a minimum in order to protect the constitutional rights of citizens to access information. Therefore, it is important in this regard that the governance structure of any legislation that seeks to supersede a constitutional obligation for open and transparent government must be sound and free from potential political interference. Moreover, there must be robust checks and balances in place which ensure that the intelligence services are not acting as both player and referee in determining what can be made secret and what remains a secret.

The argument in favour of official secrecy is that this is necessary in order to safeguard “national security”. Yet there is a much better argument for saying that public scrutiny of decisions related to defence and intelligence is likely to make for a more secure society. For example, many countries, and South Africa in particular, have a long history and experience of unaccountable intelligence services that direct their activities against domestic political opponents rather than genuine threats to national security. Freedom of information can help to curb such behaviour. Secrecy can lead to corruption and inefficiency in the security services, which in turn undermines security\textsuperscript{9}.

\textsuperscript{8} MINISTERIAL REVIEW COMMISSION ON INTELLIGENCE, FINAL REPORT TO THE MINISTER FOR INTELLIGENCE SERVICES, THE HONOURABLE MR RONNIE KASRILS, MP, 23 SEPTEMBER 2008

4. Protection of State Information and the Constitution

The Foundation’s submission on the Protection of State Information Bill seeks to examine certain of the definitions used in the Bill and the overall governance framework of the Bill as it pertains to the Constitution of South Africa.

A close reading of the Bill which was passed by the National Assembly in November 2011 highlights a number of governance failures which are logically and philosophically opposed to the idea of a Constitutional Democratic State. The Foundation has identified the Bill, in its current form, as an arbitrary exercise of state power based on the Bill’s dismally poor governance framework and ambiguous use of definitions.

The South African Constitution favours an open and transparent state where the free flow of information and the right to access that information are enshrined and protected. For the State to limit those rights, under section 36 of the Constitution, the burden falls on the State to prove that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including-

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

No law may limit any right entrenched in the Bill of Rights unless it complies with Section 36 of the Constitution.

Thus, using the Constitution as the starting point, it is clear that any limitation on a right entrenched in Chapter 2 of the Constitution must be reasonable and justifiable. The burden of defending this position falls on the State. Therefore, it is not for citizens to be forced to defend an entrenched right, but for the State to make a reasonable and justifiable case as to why it
seeks to limit a right\textsuperscript{10}. The Foundation’s concern is that the Bill, at the least, gets uncomfortably close to placing that burden of proof onto the individual and not the state. Civil society organisations, opposition political parties, business leaders, former Ministers and some senior ANC stalwarts have continually had their reservations and comments sidelined by a security cluster intent on getting this piece of legislation passed. This behaviour does not endear many to the merits of this Bill, if the perception created is one that shows a disregard to engage fully and openly on important legislative concerns.

5. General governance problems with the Protection of State Information Bill

As highlighted throughout this submission, the Foundation has identified a number of governance issues relating to the construction of this Bill. Chief among those relates to the process of classification. This concern also extends to those responsible for making the classification. In the Foundation’s view the procedures to be followed and those responsible for carrying out classification, remain too broad and may pose a significant risk to constitutionally guaranteed freedoms.

The following section of this submission outlines the concerns the Foundation has identified with this particular Bill and examines them in greater detail.

5.1 Conflation of information management with the classification of sensitive information

5.1.1 Law or conduct inconsistent with the Constitution is invalid. Obligations imposed by the Constitution must be fulfilled. The Constitution sets the parameters for the exercise of public and private power.

5.1.2 All policy must comply with the constitutional constraints of legality, rationality, and compliance with the Bill of Rights. Where policy is pursued through “administrative action”, there are two additional requirements: “what constitutes administrative action” and “what do procedural fairness and reasonableness require?”

5.1.3 Government conduct must have a legal foundation in the Constitution or legislation. The principle of legality is based on the rule of law - a founding principle in our democracy. The new order establishes a “culture of justification” – every exercise of power is expected to be justified.

5.1.4 Section 32 of the Constitution states –

“Access to information”

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.”

5.1.5 To this extent the Promotion of Access to Information Act 2 of 2000 (PAIA) was passed to give practical effect to this right. Any attempt to narrow or limit that right should be couched in the narrowest terms possible.

5.1.6 The Preamble to PAIA recognises that -

• the system of government in South Africa before 27 April 1994, amongst others, resulted in a secretive and unresponsive culture in public and private bodies which often led to an abuse of power and human rights violations;
• section 32(1)(a) of the Constitution provides that everyone has the right of access to any information held by the State;
• national legislation must be enacted to give effect to this right in section 32 of the Constitution;

5.1.7 PAIA further notes that it must be borne in mind that -

• the State must respect, protect, promote and fulfil, at least, all the rights in the Bill of Rights which is the cornerstone of democracy in South Africa;
• the right of access to any information held by a public or private body (our emphasis) may be limited to the extent that the limitations are reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom as contemplated in section 36 of the Constitution;
• reasonable legislative measures may, in terms of section 32(2) of the Constitution, be provided to alleviate the administrative and financial burden on the State in giving effect to its obligation to promote and fulfil the right of access to information
5.1.8 PAIA notes further that it should -

- foster a culture of transparency and accountability in public and private bodies by giving effect to the right of access to information;
- actively promote a society in which the people of South Africa have effective access to information to enable them to more fully exercise and protect all of their rights.

5.1.9 Given the constitutional right of access to state information and the promulgation of PAIA which was enacted to promote that right, any legislation which seeks to narrow or limit that right should be couched in the narrowest terms possible.

5.1.10 The Bill under review defines state information as any information in the possession of any organ of state. It then goes on to define “sensitive information” as information which must be protected from unlawful disclosure and to prevent the national security of South Africa from being harmed. However, sensitive information is not included in the definition of state information. There is also no definition of unlawful disclosure.

5.1.11 For information to be sensitive it has to relate to national security which is defined and largely falls within a common understanding of what national security may be. However, unless national security is at stake, sensitive information does not exist.

5.1.12 This complex of definitions makes the issue of what should be at stake clumsy and unclear. This then permeates through any attempt to interpret the rest of the Bill.

5.1.13 “Valuable information” is information contemplated in this Act whose unlawful alteration, destruction or loss is likely to deny the public or individuals of a service or benefit to which they are entitled (as defined). There appears to be little connection in the Bill to valuable information being state information or sensitive
information. This definition appears to have been inserted with no relation to the main purpose of the Bill which is to protect state information. The connection is made further on in the Bill but does not relate or appear to be related to the main purpose of the Bill.

5.1.14 There appears to be confusion between the classification of state information and the management of information that could be sensitive or embarrassing.

5.1.15 The Objects of the Bill (section 2) are to deal with state information and its classification. But the Application of the Act (section 3) is to protect valuable information. These are two completely different categories of information, dealing with two completely different ideas. The objects of the Bill have no connection with the application of the Bill. The objects of the Bill concern keeping certain information secret; the applications are to ensure that a different type of information altogether is not altered, destroyed or lost.

5.1.16 This inappropriate conflation is further illustrated by section 3 which states that the “classification, reclassification and declassification applies to the security services and the Chapter 11 oversight bodies”. The oversight bodies contemplated by section 199(8) of the Constitution, to give effect to the principles of transparency and accountability, are multi-party parliamentary committees which must have oversight of all security services in a manner determined by national legislation or the rules and orders of Parliament. The “security services” are the defence force, the police services and the intelligence services. However the Bill authorises all organs of government to classify information.

5.1.17 Section 6(a) states that unless restricted by a law that clearly sets out reasonable and objectively justified public or private considerations, state information should be available and accessible to all persons. This reflects the Bill’s relative subservience
to the Constitution and PAIA. **ALL** state information **must** be available and accessible to all **unless** classified in terms of the definitions and sections of this Act.

5.1.18 We would put forward a further argument that there may, in fact, be no such thing as secret information. It only exists as is genuinely necessitated by national security. It is a generally accepted practice, however, that state information may become classified and therefore secret.

5.1.19 Section 6(g) of the Bill recognises that **some confidentiality and secrecy** is vital to save lives, to enhance security, to protect the freedom and security of persons, bring criminals to justice, protect the national security and to engage in effective government and diplomacy. These considerations of security, by definition, are limited to those affecting “National Security” as defined and in terms of the General Principles only.

5.2 Classification Authorities

5.2.1 A “Classification Authority” is an entity or person authorised to classify state information and includes—

(a) a head of an organ of state; or

(b) any official to whom the authority to classify state information has been delegated in writing by a head of an organ of state.

This is potentially a huge number of people because “organ” is defined in section 239 of the Constitution as a “department of state or national, provincial or local administration; any functionary or institution, or sphere of government; or exercising a power or performing a function in terms of the Constitution or exercising a public power or performing a public function in terms of any a provincial constitution or legislation.” The definition excludes a court or a judicial officer.
5.2.2 The Foundation maintains that there cannot possibly be that many organs of state whose information would ever justify classification in terms of this Act. But certainly to require all of them to have the right to do so and to create separate policies on classification each is irrational. Given the fact that this legislation is an exception to a range of Constitutional freedoms, fewer rather than more government agencies should fall under it. Thus the idea of a city council head or his “senior nominee” classifying information is ludicrous.

5.2.3 In terms of section 10, **classified information** is state information which is also sensitive information which is in material or record form. **Material**, however, is not defined by the Bill and it should be if it is going to be used.

5.2.4 **Classified information**
- must be protected from **unlawful disclosure** and against alteration, destruction or loss as prescribed;
- must be safeguarded according to the degree of harm that could result from its unlawful disclosure;
- may be made accessible only to those holding an appropriate security clearance and who have a legitimate need to access the state information in order to fulfil their official duties or contractual responsibilities; and

- must be classified in terms of section 12.

Arguably, this limits the organs of state that should or could declare information as classified. However, the sweeping provision regarding eligible organs should still be narrowed considerably.

5.2.5 Section 11 provides that State information is classified in terms of section 14 when
“a classification authority has identified state information in terms of this Act as state information that warrants classification;”

5.2.6 Section 12(1) provides that State Information may be classified as confidential if the information is sensitive information, the disclosure of which is likely or could reasonably be expected to cause demonstrable harm to the national security of the Republic.

5.2.7 The concept of “Confidentiality” is introduced for the first time. It seems that confidential information is state information which is not necessarily classified but is likely to or could reasonably be expected to cause demonstrable harm to national security. How does this differ from classified information and why is it not defined and distinguished from classified information?

5.2.8 In terms of section 12 (2) state information may be classified as secret if the information is sensitive information, the disclosure of which is likely or could reasonably be expected to cause serious demonstrable harm to the national security of the Republic. Once again secret is only defined in terms of this subsection. This provision can be provided with reference to the terms defined in section 1 (Definitions). It should not be redefined here.

5.2.9 Section 12(3) provides that State information may be classified as top secret if the information is sensitive information, the disclosure of which is likely or could reasonably be expected to demonstrably cause serious or irreparable harm to the national security of the Republic. Is there value to this third category of classification? How does an official determine the relative differences between confidential, secret or top secret? Thus who is given this right to determine the relative differences, and on what basis?
5.2.10 Section 13 (Authority to classify state information) (1) provides that subject to subsection (3), any head of an organ of state may classify state information using the classification levels set out in section 12. That Head may delegate, in writing, the authority to classify to a staff member at a **sufficiently senior level**. Only designated staff members may be given the authority to classify state information as secret or top secret.

5.2.11 Classification decisions must be taken at a sufficiently senior level to ensure that only that state information which genuinely requires protection is classified. We submit that no Head of an organ of state should be entitled to classify information. The Head should only be able to motivate to an independent committee which information is to be classified. Surely classification of information is too serious to let any head of an organ of state to delegate such a task to his choice of “sufficiently senior level”?

5.2.12 Section 14 deals with “Conditions for classification and declassification”. We will refer only to certain subsections. Subsection (1) provides that the decision to classify information must be based solely on the conditions set out in this Act.

5.2.13 Subsection (2) (a) **reiterates that secrecy is justifiable only when it is necessary to protect the national security.** Further 14(2) (c) and (d) states that classification is an exceptional measure and should be classified only when there is “a clear, justifiable and legitimate need to do so; and (ii) a demonstrable need to protect the state information in the interest of the national security.”

5.2.14 Section 14(3)(c) refers to classification being needed if disclosure might “seriously and substantially impair the national interest, defence or intelligence systems, plans or activities”. There is no justification for adding **defence or intelligence.** The wording implies that defence or intelligence considerations apply over and beyond **national security** which should not be the case.
5.2.15 Similarly, section 14(3)(d) refers to information which seriously and demonstrably impairs relations between South Africa and a foreign government, or seriously and demonstrably undermines on-going diplomatic activities of the Republic. Again, the only criterion should be national security.

5.2.16 Section 15 provides that a person who is in possession of a classified record knowing that such record has been unlawfully communicated, delivered or made available other than in the manner and for the purposes contemplated in this Act, except where such possession is for any purpose and in any manner authorised by law, must report such possession and return such record to a member of the South African Police Service or the Agency to be dealt with in the prescribed manner.

5.2.17 The Bill neither defines nor describes “unlawful communication”. Even if it did, it should be up to the relevant classification authority to keep the information secret. The authority is entitled to impose such restrictions on the actions of an employee with regard to the disclosure as are permitted by labour law, criminal law and the common law.

5.2.18 The Foundation submits that it’s up to the classification authority itself must keep information secret in terms of the Act and its rules or policy. If the information then gets into the public domain, it is no longer secret even if is classified. Action can then be taken against the leaker of the information. Action should not be taken against the recipient. It is up to the authority and its employees to keep information secret. If they fail it is no longer a secret. It is unreasonable to expect any one outside those auspices to be responsible. The outsider can be charged with treason, defamation etc.
5.3 **Offences and Penalties Chapter 11**

5.3.1 The subtitle to this chapter is “Espionage offences”. Although “espionage” is not defined each section does refer to making information known which the informer knows or ought reasonably to have known would directly or indirectly benefit a foreign state.

5.3.2 There is no reference to the benefit to the foreign state being simultaneously detrimental to South Africa or whether that state has negative intentions towards South Africa which would in any way be affected by the possession of such information.

5.3.3 Although these criminal sanctions would only be considered on rare occasions, it seems unduly harsh to set minimum sanctions.

5.3.4 We submit that espionage and the offences relating thereto should not be contained in this legislation. Although there may be a connection it is too heavy handed to deal with espionage in this Bill as what appears to be an afterthought. The same applies to sections 37, 38 and 39.

5.3.5 Similarly, sections 41 and 42 which deal with the operation of foreign secret agents are inappropriate in this piece of legislation. The section does not deal directly with state information and its classification or otherwise.

5.4 **Prohibition of Disclosure – section 49**

5.4.1 Given our prior arguments, the Foundation has grave reservations about penalising the public for publishing or otherwise distributing information relating to a “state security matter”.


5.4.2 It forces the citizenry who first and foremost have a constitutional right to access to information, to become the guardians of the state’s carelessness in how it manages its classified information. This is aggravated if the information has been classified improperly and at the time of publication this has not been established;

5.4.3 Given the confusion with regard to the purposes of the Bill, by conflating the classification of information with the management of information, a citizen may be punished for contravening of a law that infringes the right to access to information in an unduly and unwarranted manner.

As this section details the current construction of this Bill, if passed unchanged, it will have the chilling effect of limiting transparency and curtailing the flow of information between departments, organs of state and the citizens of the country.

While the Bill stipulates regular reviews of classified information, it is the Foundation’s concern that due to the high number of people with the power to classify under this Bill, the sheer volume of the information to be reviewed will inhibit its successful review. This will result in backlogs and time delays and hence undermine the entire process. The effect of this will be to further undermine the constitutional imperative of free information flows, which may also unintentionally hinder aspects of service delivery from the national level of government down to the municipal level.

While the Classification Review Panel is a welcome sight, upon closer inspection it falls short of a truly independent review mechanism tasked with providing oversight to classification decisions.

- First, it is reactive in nature in that it may only respond once a classification decision has been taken by one (of potentially thousands) of authorised personnel. This process curtails its review functions.
- Secondly, its appointment and composition remains in the ambit of the security cluster. Section 22(2) of the Bill stipulates that [t]he Joint Standing Committee on
Intelligence must table a list of five persons for approval by the National Assembly. Section 22(7) then places a further limit on who may be appointed to the Review Panel by requiring of that person that they hold a valid security clearance issued by the Ministry of State Security.

By formulating this aspect of the Bill in this way, the Security Ministry is able to wield a significant, if not overwhelming, influence in determining who finally gets appointed to the panel. This in turn undermines the accountability function that this panel should be enforcing. Ultimately, it becomes impossible for the general public, civil society organisations, the media or other interested parties to gain effective access to certain information which may be classified. This in turn undermines the constitutionality of the freedom to access state information.

These examples highlight a poor governance framework which permeates the Bill. The Foundation is concerned that this Bill will place a significant amount of power in the Minister’s office, without placing a proportionate level of protection and accountability on the process to ensure that the constitutional right of freedom of expression is protected.
6 Conclusion

The right of freedom of expression is universally accepted as a fundamental right. However, it is not an absolute right and all the international treaties and covenants which deal with it accept that it may be limited in certain, precisely defined, circumstances. Article 19, an international organisation that defends freedom of expression and information, has articulated a three part test when bodies determine a limitation on the right to freedom of expression. We submit their arguments as the basis of our conclusion.

6.1 Part one – Provided by Law

The first condition means, first and foremost, that an interference with the right to freedom of expression cannot be merely the result of the whim of a public official. There must be an enacted law or regulation which the official is applying. In other words, only restrictions which have been officially and formally recognised by those entrusted with law-making capacity can be legitimate.

The condition of ‘provided by law’ requires more, however, than the mere existence of a written piece of legislation. The legislation must also meet certain standards of clarity and precision, enabling citizens to foresee the consequences of their conduct on the basis of the law. Vaguely worded edicts, whose scope of application is unclear, will not meet this standard and are thus illegitimate restrictions on freedom of expression.

6.2 Part two – Legitimate Aim

The second requirement for restrictions on freedom of expression is that they must serve a legitimate aim. This requirement is not open-ended; the list of legitimate aims provided in Article 19(3) of the International Covenant on Civil and Political Rights is exclusive and governments may not add to these. It includes only the following legitimate aims: respect for the rights and reputations of others, and protection of national security, public order (ordre public), public health or morals.
The rationale of this part of the test is to make it clear that not all of the motives underlying governments’ decisions to restrict freedom of expression are compatible with a democratic form of government. For example, a desire to shield a government from criticism can never justify limitations on free speech. In order to satisfy this second part of the test, a legal provision which limits freedom of expression must serve a legitimate aim both in purpose and in effect. It is not sufficient if the provision has an incidental effect on one of the legitimate aims; if the purpose of enacting it was to serve another aim, it will not pass this part of the test.

6.3 Part three – Necessity

The final part of the test holds that even if a restriction is in accordance with an acceptably clear law and if it is in the service of a legitimate aim, it will still breach the right to freedom of expression unless it is truly necessary for the protection of that legitimate aim. This part of the test may seem self-evident: if a restriction on a right is not needed, why impose it?

To justify a measure which interferes with free speech, a government must be acting in response to a pressing social need, not merely out of convenience. On the continuum between ‘useful’ and ‘indispensable’, the meaning of ‘necessary’ should not be placed in the middle, but close to the ‘indispensable’ end. If there exists an alternative measure which would accomplish the same goal in a way is less intrusive to the right to free expression, the chosen measure is not in fact ‘necessary’. The impact of restrictions must be proportionate, meaning that the harm to freedom of expression caused by a restriction must not outweigh its benefits to the interest it is directed at\(^1\).

6.4 Considering this submission in its entirety and using this three-part test as a means of determining the merits of this Bill, the Helen Suzman Foundation contends that this Bill fails at a number of levels.

6.5 As argued earlier the Bill clearly conflates two different issues – effective information management on behalf of the state and a classification regime. The problem in conflating these two distinct areas of concern is that the Bill uses vague, broad and conflicting language and attempts to rely on national security imperatives to legitimize it.

6.6 The problem with this broad use of national security imperatives is that it leaves the Bill open to manipulation and political interference, thus undermining key constitutional imperatives in favour of an open, transparent and responsive government.

6.7 Finally, it should be noted that the Foundation has not, in this submission, addressed the public interest defence. Should the Bill proceed in its present form, the Foundation intends to address this vital question in the appropriate forum, namely by approaching the Constitutional Court to establish legal clarity on this matter.