SUBMISSIONS TO THE AD HOC COMMITTEE ON THE PROTECTION OF STATE INFORMATION BILL (NATIONAL COUNCIL OF PROVINCES) REGARDING THE PROTECTION OF INFORMATION BILL B 6B – 2010

SUBMITTED ON BEHALF OF PRINT MEDIA SOUTH AFRICA AND THE SOUTH AFRICAN NATIONAL EDITORS' FORUM

17 February 2012

The Committee is requested to note that the parties wish to make an oral presentation during the hearings

South African National Editors' Forum
SANEF

PRINT MEDIA
South Africa

WEBBER WENTZEL

ALN

EXECUTIVE SUMMARY

1. **Introduction**

1.1 SANEF and PMSA submit that aspects of the Protection of Information Bill B 6B-2010 ("**the Bill**") are unconstitutional in that they offend the values of openness, accountability and transparency underlying the Constitution, and the constitutional rights to freedom of expression and access to information.

1.2 It is undoubtedly the case that the topics dealt with in the Bill are of great significance to our democracy. The drafters of the Bill deserve credit for crafting proposed legislation that is different to the apartheid-era Protection of Information Act 84 of 1982. However, the Bill suffers from fundamental constitutional flaws.

2. **The constitutional background**

2.1 The values of openness, accountability and transparency are underlying values of the Constitution of the Republic of South Africa 108 of 1996 ("**the Constitution**").

2.2 The importance of freedom of expression to an open and democratic society, and particularly the role of the media in a democracy, has been reiterated by our highest courts on numerous occasions. It is significant that the guarantee of media freedom is designed to serve the interest that all citizens have in the free flow of information which is possible only if there is a free press.

2.3 The Constitution also protects the right of access to information in section 32. The Promotion of Access to Information Act 2 of 2000 ("**PAIA**") was promulgated to give effect to the constitutional right of access to information.

2.4 It is trite that no right is absolute. The rights to freedom of expression, and access to information may yield to more compelling state interests. PMSA and SANEF accept that one such compelling state interest is the protection of national security. It is legitimate for national security interests to justifiably limit rights but the burden of justification in this context is firmly upon the state. Provisions of the Bill that limit the rights to freedom of expression and access to information will therefore not survive constitutional scrutiny unless these restrictions comply with section 36 of the Constitution.

3. **Criminal offences that undermine media freedom**

3.1 SANEF and PMSA submit that a number of the criminal offences set out in the Bill are unconstitutional in that they disproportionately limit the right of access to information and freedom of expression (including media freedom). These offences include:

3.1.1 clause 36 of the Bill which creates the espionage offence;

3.1.2 clause 37 which creates the offence of receiving state information;

3.1.3 clause 38, which creates the hostile activity offence;

3.1.4 clause 40(1), which makes it an offence to intentionally access classified information;

3.1.5 clause 43, which creates the offence of disclosing classified information;

3.1.6 clause 44, which makes it an offence to fail to comply with clause 15. Clause 15 in turn requires each person to return any classified information in their possession to the South African Police Service; and

3.1.7 Clause 49, which makes it an offence to disclose a “state security matter”.

3.2 SANEF and PMSA submit that the main constitutional difficulties that arise from these offences from a media perspective are the following:

3.2.1 The offences created in clauses, 36, 37, 38 and 39 are inconsistent with the common law principle that conduct is not unlawful unless committed with a guilty mind. The effect of the words "knows or ought reasonably to know", which are used in each of these clauses, is that each of these offences can be committed even if the accused does not have <u>actual</u> knowledge. The Bill should require that the accused needs to have committed the crime with knowledge of its illegality, including that he or she was disclosing classified information, and <u>with the intention to cause substantial harm to national security</u>.

3.2.2 The Bill does not provide for an <u>explicit public interest defence</u>. SANEF and PMSA submit that the case for a public interest defence is overwhelming. Such a defence would allow a whistleblower or journalist who publishes classified information to argue that the disclosure was justified, for instance

because it revealed evidence of significant incompetence, criminality, wrongdoing, abuse of authority or hypocrisy on the part of government officials. The failure to provide for a defence of public interest coupled with the vagaries of the offences created and the severe penalties involved will undoubtedly create an unjustifiable chilling effect on freedom of expression.

3.2.3 The Bill should also be amended to include a public domain defence. This defence postulates that where the information is already in the public domain, future restrictions on its publication would be futile. We submit that it would not be correct to argue that harm to national security would likely ensue from the republication of information that is already in the public domain.

3.2.4 A number of the criminal offences clauses in the Bill fail to recognise the maxim *ne bis in idem* which provides that no person can be tried for the same offence twice. This is recognised in the section 35(3) of the Constitution and section 106(1)(c) of the Criminal Procedure Act 51 of 1997. The offences created in clause 49 (disclosure of state security matter) and clause 43 (the general disclosure offence) overlap and therefore when a person commits an offence such person will also commit an offence under clause 43. Furthermore, if one has regard to the offences created in clauses 49(c), 44 and 37, a person could be subject to three separate sentences if they are in possession of information that relates to a 'state security matter'.

4. Overbroad definitions

National security and State Security Matter

4.1 PMSA and SANEF submit that the definition of "national security" and "state "security matter" may still be overbroad. The main problem in regard to the definitions is the use of the word "includes". It is unclear whether the word "includes" was deliberately inserted to indicate that the matters listed in the definition are not exhaustive or whether this was a drafting oversight. SANEF and PMSA submit that this use of the word “includes” renders the above definitions overbroad and unworkable and consequently it should be deleted from both definitions.

5. **Classification of information by members of the security services**

5.1 Clause 13(6) empowers every member of the security services as contemplated in chapter 11 of the Constitution to classify information, subject to confirmation by the head of the organ of state in question. No attempt is made to confine the said authority to classify information to members of the security services with a particular rank. This flies in the face of the general principle in clause 13(4) of the Bill that information must be classified at a sufficiently senior level.

5.2 The review of classified information by the head of the organ of state concerned does not remedy the problems created by clause 13(6) because it is not clear how soon the review must take place after the classification decision is made.

5.3 Section 13(6) carries potential for abuse and we submit that the section must be deleted from the Bill.

6. **Classification of whole document when only part classifiable**

6.1 Having regard to the presumption of openness as reflected in section 32 of the Constitution, the founding values of accountability and openness and the requirement that legislation adopt the least restrictive means possible in terms of section 36(1)(e) of the Constitution, we submit that the Constitution requires that information should only be kept away from the public to the limited extent that it is necessary to achieve specified national security objectives.

6.2 For that reason, the legislation ought to require that any information in a record that is not protected and that can reasonably be severed from the protected parts of the record must be severed and disclosed.

7. **Categories of classified information**

7.1 The accessibility of information to members of the public and disclosure of information is drastically limited once the information is classified. SANEF and PMSA submit that the inclusion of the method of bulk classification provided in clause 13(5) will result in the decision maker being absolved from the responsibility to consider and apply their mind to all the specific records which fall within that category and is dangerously restrictive of access to information and free speech.

8. **Request for access to classified information and status review**

8.1 SANEF and PMSA are of the view that the circumstances under which information can be declassified under clause 19(3) are too narrow and amount to an unjustifiable limitation on the right to access information. Clause 19(3) should be amended to state that, in addition to the factors already set out in that clause, when a request is made for information to be declassified, the information will be evaluated afresh and if it is found that it does not meet the criteria for classification (and ought never to have been classified in the first place), it will be declassified.

9. **The powers of courts and the open justice principle**

9.1 Clause 52 of the Bill provides that where classified information is placed before a court, such information may not be disclosed to the public unless the court orders such disclosure.[1] Before making such an order, the Court is required to take reasonable steps to receive submissions from the party that classified the document or the Director – General of the Agency.[2]

9.2 However, the Court is given a discretion about whether to require information from any other interested party.[3] We submit that this is problematic. Given the well-established open justice principle, where a Court may withhold information from the public, it is imperative that all interested parties be afforded the opportunity to be heard.

10. **The offence of accessing a state owned computer**

10.1 The offences created under clauses 40(6) (b) - (d) do not appear to be directly relevant to the Bill and create criminal sanctions in respect of conduct which may be harmless or otherwise lawful. The definition of "access to a computer" is so broad that merely accessing a flash drive owned by the state, regardless of whether it contains classified information, could result in an offence being committed. We submit that clause 40(6)(b) should be amended to specify that the computer must be accessed with the intention to access information which the accused was not lawfully entitled to receive.

---

[1] Clause 52(1)(a)
[2] Clause 52(4)
[3] Clause 52(6)

11. **Conclusion**

11.1 We submit that the Bill is in many respects a welcome change to the national security landscape in South Africa. The Bill has the potential to play a significant role in transforming our society from a culture of secrecy and repression to one of transparency, accountability and responsiveness, and to become a leading precedent for open and democratic governments the world over. To achieve these goals and the desirable objectives it articulates, the Bill must properly respect openness, free speech, and access to information, in the various ways that we have suggested.

FULL LENGTH SUBMISSIONS

1. **Introduction**

1.1 These submissions on the Protection of State Information Bill B 6B-2010 ("**the Bill**") are made on behalf of Print Media South Africa ("**PMSA**") and The South African National Editors' Forum ("**SANEF**").

1.2 PMSA is an umbrella body that represents the interests of the print media industry in South Africa. The primary objective of PMSA is to provide a forum for unified representation of its members at industry level in respect of all matters that affect the print media. It represents over 700 newspaper and magazine titles across South Africa.

1.3 SANEF is a non-profit organisation whose members include editors, senior journalists and journalism trainers from all areas of the South African media. SANEF's primary aim is to be a representative and credible voice of journalism in society, to facilitate diversity in newsrooms and reporting, enable a culture of real debate and promote free and independent journalism of the highest standard.

2. **Background**

2.1 Webber Wentzel, on behalf of PMSA, made submissions on the 2010 Bill whilst it was before the Ad Hoc Committee on the Protection of Information Bill ("**the Ad Hoc Committee**"). We attach a copy of the executive summary of the submission as Annexure "A". A copy of the full submission will be made available should the committee believe that this would be useful.

2.2 Webber Wentzel, on behalf of SANEF and PMSA, also made submissions to the ANC Information Bill Committee. We attach a copy of the executive summary of this submission as Annexure "B". A copy of the full submission will be made available should the committee believe that this would be useful.

2.3 The Bill was approved by the Ad Hoc Committee and adopted on Monday 6 September 2011.

2.4 As a starting point we note that some of the problematic aspects of the Bill which were addressed in the 2010 submissions made on behalf of PMSA have been

rectified in the final version of the Bill. PMSA and SANEF appreciate the continued engagement with the public on this matter.

2.5 Despite some of the positive developments in the Bill, PMSA and SANEF are of the view that there are a number of changes that ought to be made in order to ensure greater protection of the public's right of access to information, as is constitutionally mandated. Our submissions are structured as follows:

2.5.1 first, we briefly set out the South African legal background against which the Bill's constitutionality must be assessed;

2.5.2 secondly, we analyse aspects of the Bill that SANEF and PMSA contend are problematic and should be amended:

2.5.2.1 the various criminal offences that would affect citizens who wish to disclose information of public interest;

2.5.2.2 the lack of a public interest and public domain defence;

2.5.2.3 the over-breadth of the definitions of *national security* and *state security matter*;

2.5.2.4 powers given to security operatives to classify information;

2.5.2.5 failure to require severability of non-classified information

2.5.2.6 bulk classification of information;

2.5.2.7 the powers of courts and the open justice principle;

2.5.2.8 requests for access to classified information and status review; and

2.5.2.9 the offence of accessing a state owned computer.

3. **The constitutional background**

3.1 Any assessment of the Bill must take into account the constitutionally protected rights which are affected by the regime of classification and protection classified information created by the Bill. The relevant rights in this regard are the right to freedom of expression and the right of access to information.

3.2 **The right to freedom of expression and of the media**

3.2.1 Freedom of expression is protected by section 16(1) of the Constitution:

> **(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** …

3.2.2 The importance of freedom of expression to an open and democratic society has been reiterated by our courts on numerous occasions. Freedom of the media – expressly protected by section 16(1)(a) of the Constitution – is inextricably connected with the right of the public to receive information and ideas (protected in section 16(1)(b) of the Constitution). It is an aspect of the right to freedom of expression that has received specific emphasis in the judgments of our highest courts:

3.2.2.1 in **Khumalo v Holomisa**,[4] the Constitutional Court stated as follows:

> **The print, broadcast and electronic media have a particular role in the protection of freedom of expression in our society. Every citizen has the right to freedom of the press and the media and the right to receive information and ideas. The media are key agents in ensuring that these aspects of the rights to freedom of information are respected.**[5]

3.2.2.2 The Supreme Court of Appeal has also articulated the importance of media freedom in our democracy. In **National Media v Bogoshi**[6], the Court held that:

> **[W]e must not forget that it is the right, and indeed a vital function, of the press to make available to the community information and criticism about every aspect of public, political, social and economic activity and thus to contribute to the formation of public opinion …. The press and the rest of the media provide the means by which useful, and sometimes vital, information about the daily affairs of the nation is conveyed to its citizens …**[7]

3.2.3 Finally, it bears emphasis that government information, such as that regulated by the Bill, constitutes political speech that lies at the core of any freedom of expression guarantee, and hence ought to receive heightened protection in our law. Restrictions on this type of speech – unlike, for

---

[4] 2002 (5) SA 401 (CC).
[5] At para 22.
[6] 1998 (4) SA 1195 (SCA).
[7] At p1209.

instance, advertisements, pornographic images or celebrity gossip – impact directly on the nature of our democracy and such restrictions must be compelling to pass constitutional scrutiny.[8]

3.3 **The right of access to information**

3.3.1 Section 32(1) of the Constitution provides as follows:

> **(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 access or protection of any rights.**

3.3.2 The Promotion of Access to Information Act 2 of 2000 ("**PAIA**") was promulgated to give effect to the constitutional right of access to information. In terms of section 11 of PAIA, a requester must be given access to a record of a public body if the procedural requirements of PAIA are complied with, and access to the record is not refused in terms of a ground of refusal set out in PAIA. There is therefore a presumption of access to information held by public bodies, subject to their entitlement to invoke a ground of refusal recognised under PAIA to resist the provision of access to the information.

3.3.3 As was enunciated by Cameron J in **Van Niekerk v Pretoria City Council**:[9]

> **In my view, s 23 [the predecessor to section 32 of the Constitution] entails that public authorities are no longer permitted to "play possum" with members of the public … The purpose of the Constitution, as manifested in s 23, is to subordinate the organs of State . . . to a new regime of openness and fair dealing with the public.**

3.3.4 And in **Brummer v Minister of Social Development and Others (South African History Archives Trust and South African Human Rights Commission as Amici Curiae)**,[10] the Constitutional Court stated the following concerning the importance of the right of access to information in our democracy:

> **The importance of this right [the right of access to information] too, in a country which is founded on values of accountability, responsiveness and openness, cannot be gainsaid. To give effect to these founding values, the public must have access to information held by the state. Indeed one of the basic values and principles governing public**

---

[8] E Barendt *Freedom of Speech* (2nd edn, 2006) at 193.

[9] 1997 (3) SA 839 (T) at 850.

[10] 2009 (6) SA 323 (CC).

> **administration is transparency. And the Constitution demands that transparency "must be fostered by providing the public with timely, accessible and accurate information."**
>
> **Apart from this, access to information is fundamental to the realisation of the rights guaranteed in the Bill of Rights. For example, 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.**[11]

3.4 **National security as a limitation on constitutional rights**

3.4.1 It is trite that no right is absolute. The rights to freedom of expression, and access to information may yield to more compelling state interests. PMSA and SANEF accept that one such compelling state interest that is in principle capable of legitimately restricting the constitutional rights of free speech and access to information, is the protection of national security.

3.4.2 The point of departure with respect to the Bill is that, although in principle it is legitimate for national security interests to justifiably limit rights, the burden of justification in this context is firmly upon the state. Provisions of the Bill that limit the rights to freedom of expression and access to information will therefore not survive constitutional scrutiny unless these restrictions comply with section 36 of the Constitution.

4. **Criminal offences that undermine media freedom**

4.1 SANEF and PMSA submit that a number of the criminal offences set out in the Bill are unconstitutional in that they disproportionately limit the right of access to information and freedom of expression (including media freedom). A number of criminal offences are capable of application to investigative journalists and citizens who disclose information of public importance :

4.1.1 clause 36 makes it an offence to unlawfully and intentionally communicate, deliver, make available, obtain, collect or capture classified information which a person "**knows or ought reasonably to have known would directly or indirectly benefit a foreign state**";

---

[11] At para 63 and 64.

4.1.2 Clause 37 makes it an offence to receive classified information which a person "**knows or ought reasonably to have known would directly or indirectly benefit a foreign state** ";

4.1.3 Clause 38 makes it an offence to unlawfully and intentionally communicate, deliver, make available, obtain, collect or capture classified information which a person "**knows or ought reasonably to have known would directly or indirectly benefit a non state actor engaged in hostile activity or prejudice the national security of the Republic**"

4.1.4 Clause 40(1) makes it an offence to intentionally access classified information without authority to do so;

4.1.5 Clause 43 makes it an offence to unlawfully and intentionally disclose classified information;

4.1.6 Clause 44 makes it an offence to fail to comply with clause 15, which in turn requires each person to return any classified information in their possession to the South African Police Service; and

4.1.7 Clause 49 makes it an offence to intentionally disclose, publish, retain and neglect to take proper care of information which the person "**knows or reasonably should know"** is a state security matter.

The absence of an appropriate *mens rea* requirement

4.1.8 The offences created in clauses, 36, 37, 38 and 39 are inconsistent with the common law principle that conduct is not unlawful unless committed with a guilty mind.[12]

4.1.9 In the Constitutional Court's decision in **S v Coetzee,**[13] the Court affirmed the pre-eminence of fault as a requirement for criminal liability. O'Regan J held that it is a fundamental principle of democratic societies that **"*people who are not at fault should not be deprived of their freedom*".**[14]

4.1.10 The effect of the words "knows or ought reasonably to know" is that each of these offences can be committed even if the accused does not have actual

[12] J Burchell *Principles of Criminal Law* (3rd ed, 2005) at 151.
[13] **S v Coetzee** 1997 (3) SA 527 (CC).
[14] At para 176.

knowledge. The negative effect of these clauses is exacerbated by the fact that in respect of clauses 36, 37 and 38, the benefit to the other state or to a non-state actor can either be direct or indirect.

4.1.11 We note that the words "unlawfully and intentionally" have been included in each of the above clauses. This appears to have been done by the Ad Hoc Committee in an attempt to address the fault requirement. However, in respect of each of the problematic clauses the words "intentionally and unlawfully" are attached to the action of communicating, receiving or disclosing information and not to the consequences that the person intended their actions to have. It appears that could be the result of a drafting error and that it can be remedied by redrafting the clauses.

4.1.12 PMSA and SANEF submit that the problem with the clauses can be cured by:

4.1.12.1 deleting the words "**out reasonably to have known**";

4.1.12.2 deleting the reference to "**indirect**" benefit to a foreign state or non state actor engaged in hostile activity; and

4.1.12.3 making it clear that the information must have been disclosed with the intention to directly benefit a foreign state or non state actor.

4.2 The above amendments will ensure that criminal consequences will ensue only in a case where actual knowledge is present and there was a clear intention to act unlawfully. It will also ensure that these offences cannot be used to prosecute ordinary citizens or journalists who have no intention to engage in espionage or hostile activities against the state.

Double Jeopardy

4.2.1 The maxim *ne bis in idem* which provides that no person can be tried for the same offence twice, is recognised in the section 35(3) of the final Constitution and section 106 (1) (c) of the Criminal Procedure Act 51 of 1997. The maxim was re-affirmed in **S v Basson**[15] where Ackermann J held that the protection against double jeopardy is one of the fundamental rights protected by the Constitution.

[15] 2005 (1) SA 171 (CC) at Para 248-254

4.2.2 Protection against double jeopardy is recognised in most democratic countries. The US Supreme Court has held that being found guilty and punished for two different crimes in respect of the same conduct is impermissible and the prohibition on this forms part of the double jeopardy principle.[16]

4.2.3 The offences created in clause 49 (disclosure of state security matter) and clause 43 (the general disclosure offence) overlap and therefore when a person commits an offence such person will also commit an offence under clause 43. The person will therefore be in a position where he or she can be punished twice in respect of the same crime.

4.2.4 Furthermore, a person could be subject to three separate sentences if they are in possession of information that relates to a 'state security matter'. In terms of clause 49(c), it is an offence to retain information pertaining to a state security matter; in terms of clause 44 failure to report classified information in your possession and return it to the SAPS is also an offence; and clause 37 creates the offence of receiving classified information which would directly or indirectly benefit a foreign state.

4.2.5 PMSA and SANEF submit that the offences in the Bill should be streamlined to avoid unnecessary duplications. In particular, clause 49 is not necessary in light of the fact that the same conduct dealt with in clause 49 can be punished under clause 43 and 44.

5. **The need for a public interest defence**

5.1 In probably the most significant omission from the perspective of media freedom and the constitutional imperative of holding the government to account, the Bill does not provide for an explicit public interest defence to any of the offences we have outlined (nor is such a defence implicit). SANEF and PMSA submit that the case for a public interest defence is overwhelming. Such a defence would allow a whistleblower or journalist who publishes classified information to argue that the disclosure was justified, for instance because it revealed evidence of significant incompetence, criminality, wrongdoing, abuse of authority or hypocrisy on the part of government officials.

---

[16] **United States v Di Francesco** 449 US 117 (1980); **United States v Dixon** 509 US 688 (1993); **Witte v United States** 515 US 389 (1995)

5.2 We submit that public interest is already a defence in a number of contexts in our law that are analogous:

5.2.1 **Section 46 of PAIA** governs the mandatory disclosure of information in the public interest. It states as follows:

> ***Despite any other provision of this Chapter, the*** **information officer of a public body must grant a request for access to a record of the body contemplated in… section 41(1)(a) or (b), if:**
>
> **(a)the disclosure of the record would reveal evidence of —**
>
> **(i) a substantial contravention of, or failure to comply with, the law; or**
>
> **(ii) an imminent and serious public safety or environmental risk; and**
>
> **(b) the public interest in the disclosure of the record clearly outweighs the harm contemplated in the provision in question.**

5.2.2 The effect of this provision of PAIA is that, inter alia, section 41 (the provision that regulates the disclosure of records concerning defence, security and international relation) may be overridden if it is in the public interest. We contend that, if documents can be released under PAIA in the public interest despite the threat that the contents pose to national security, it would be anomalous and inequitable in parallel circumstances to criminalise the access, disclosure and continued possession of classified documents that are significant for the public.[17]

5.2.3 That a publication is in the public interest already functions as a defence to an infringement of privacy at common law, even in circumstances where the media has obtained the information illegally. In **Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another**,[18] 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**

---

[17] Although the Bill pays lip service to the considerations under section 46 of PAIA, we submit that this is inadequate. See paragraph 10 below.

[18] 1993 (2) SA 451 (A).

> **of the information should be permitted, despite its source or the manner in which it was obtained.**[19]

5.2.4 It is submitted that the decision of Yacoob J in **Independent Newspapers (Pty) Ltd v Minister for Intelligence Services**[20] is compelling in this context. The case was not concerned with criminal liability on the part of the media for publishing classified documents, but rather whether such documents should be made public. The decision of Yacoob J nevertheless illustrates the potency of a public interest-based analysis in national security cases:

> **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…**[21]
>
> **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. …** [22]
>
> **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.** [23]

5.2.5 We note that a reference to the Protected Disclosures Act ("**PDA**") has been included in clause 43(a) of the Bill. Whilst the inclusion of the PDA is a (very small) step in the right direction, it does not resolve the need for a public interest defense for the following reasons:

5.2.5.1 The protection extended by the PDA only relates to individuals who are employed by an organization. The definition of "employee" under the

---

[19] At 463. See also **MEC for Health, Mpumulanga v M-Net** 2002 (6) SA 714 (T) at para 27.
[20] 2008 (4) SA 31 (CC) ("**the Masetlha case**").
[21] At para 88.
[22] At para 103.
[23] 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.

PDA specifically excludes independent contractors.[24] This means, for example, that if an individual receives a tender to conduct certain work for a government department and in the process of conducting that work acquires knowledge about unlawful activities that have been classified, the individual concerned would not be able to rely on the PDA as a defence;

5.2.5.2 The definition of "protected disclosure" contained in the PDA specifically excludes a disclosure in respect of which "the employee concerned commits an offence by making that disclosure". Since clause 43 of the Bill makes it an offence to disclose classified information and there are various other offences relating to receiving, possessing and disclosing classified information contained elsewhere in the Bill, it is unclear how the PDA is to be reconciled with clause 43(a);

5.2.5.3 The PDA is only included as a defence under clause 43 of the Bill. This means that a whistleblower can potentially still be targeted under clause 49, if the disclosure relates to a state security matter, or clauses 37 and 38, given the overbroad wording in those clauses;

5.2.5.4 The defence relating to the PDA does not (and is clearly not intended to) cover journalists or concerned citizens who are not employees but who receive classified information of public importance. Accordingly, it would not be open to such a person to claim that he should not be criminally liable because the information he published was provided by a whistleblower in accordance with the PDA. Section 9 of the PDA permits a whistleblower to approach any person, which includes the media, to expose wrongdoing if the other (quite onerous) channels of disclosure set out in the PDA have not worked. The fact that journalists who publish material disclosed in accordance with section 9 of the PDA can be prosecuted in any event undermines the purported protection afforded to whistleblowers under this section.

5.2.6 Three of the most prominent concerns regarding the inclusion of a public interest defence that have been expressed during the course of the

[24] See section 1 of the PDA.

Parliamentary debates on the bill in the past few years warrant further consideration:

5.2.6.1 The idea that including a public interest defence would create legal uncertainty. SANEF and PMSA submit that this concern is misplaced because, as set out above, our courts are well versed in applying the public interest defence in a range of contexts in our law and would accordingly be able to develop similar jurisprudence to address any public interest defence included in the Bill. In any event, the desire to create legal certainty cannot outweigh the public and the media's constitutional right to freedom of expression and access to information;

5.2.6.2 It has also been suggested that a public interest defence is unnecessary because such a defence already exists under the common law or that a court would not find someone guilty if that person was exposing wrongdoing. These suggestions are, with respect, incorrect. There is no general common law defence of 'public interest' which is available to a person accused of committing a statutory offence. If a public interest defence is not specifically included in the Bill it will not be open to the public and the media to raise such a defence;

5.2.6.3 The idea that citizens must use the 'correct channels' to access information by requesting that the information be declassified once they become aware of its existence. There are a number of problems with this approach. Firstly it fails to take into account the possibility that once such a citizen reports the communication of classified information and returns that information (as required by clause 15) it would lead to an investigation to uncover and potentially silence the citizen's source. It also fails to take into account the potential for information to be destroyed once enquires have been made by journalists. Such a procedure provides fertile ground for enabling a cover-up in circumstances where the citizen is prohibited from making public any knowledge that he or she has about the classified information pending the decision to declassify.

5.2.7 SANEF and PMSA submit that the failure to provide for a defence of public interest coupled with the vagaries of the offences created and the severe penalties involved, will undoubtedly create an unjustifiable chilling effect on

freedom of expression. This will drastically undermine public discourse, discussion and debate on matters of political speech, which ought to receive heightened protection.

6. **The public domain defence**

6.1 The Bill should also be amended to allow the media to argue the defence of public domain. This defence postulates that where the information is already in the public domain, future restrictions on its publication would be futile. In such circumstances, we submit that it would not be correct to argue that harm to national security would likely ensue from the republication of the information. It cannot be competent to convict, for instance, a journalist or citizen who publishes classified information in circumstances where the information is already in the public domain, as a result of a disclosure by someone other than the re-publisher himself or herself.[25] SANEF and PMSA accept that the public domain defence would not avail the party who *first* places the material in the public domain, but that ought not to limit the rights of members of the public to republish the information.

6.2 The public domain doctrine in this context is well-rehearsed in international law and is also acknowledged in our jurisprudence. We begin with the position in South African law and then discuss a few of the leading cases in England and in the jurisprudence of the European Court of Human Rights.

South Africa

6.3 It is basic to the principle of confidentiality that information cannot be protected once it loses its secrecy. This is recognised in section 37(2)(a) of PAIA, which provides that, although an information officer of a public body may in general refuse a request for access to a record if the disclosure of the record would constitute an action for breach of a duty of confidence, he or she may not refuse to disclose if the records consists of information "*already publicly available*". The principle is also recognised in South African law relating to commercial confidentiality,[26] and in our law of privacy.[27]

---

[25] We submit that it matters not whether the public domain principle is regarded as a defence to the crime or a factor that negatives harm.

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

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

6.4 The Constitutional Court has also recognised that the concept of public domain is an important factor in determining whether classified documents before a court should be released to the public. In **Masetlha**, Moseneke DCJ for the majority of the Court held:

> **In deciding whether documents ought to be disclosed or not, a court will have regard to all germane factors which include the nature of the proceedings; the extent and character of the materials sought to be kept confidential; the connection of the information to national security; the grounds advanced for claiming disclosure or for refusing it; whether the information is already in the public domain and if so, in what circumstances it reached the public domain; for how long and to what extent it has been in the public domain; and, finally, the impact of the disclosure or non-disclosure on the ultimate fairness of the proceedings before a court. These factors are neither comprehensive nor dispositive of the enquiry.[28] (our emphasis)**

6.5 Also in the **Masetlha** case, Yacoob J held:

> **If the information is already lawfully in the public domain there can, in my view, be no reason for its non-disclosure.[29] (our emphasis).**
>
> **And later:**
>
> **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. [30] (our emphasis)**

The United Kingdom and the European Court of Human Rights

6.6 The public domain doctrine in the context of national security restrictions has been especially prominent in the jurisprudence of the English courts and in the European Court of Human Rights.

6.6.1 The leading case is the famous case of **Attorney-General v Guardian Newspapers (No 2)** ("**the Spycatcher case**"), where the House of Lords was requested by the government to interdict the distribution of a book by a former MI5 agent, the contents of which contained names of colleagues, details of operational techniques, and of specific operations (including a plan

---

[28] **Masethla** at para 55.
[29] At para 91.
[30] At para 103.

by MI6 to assassinate President Nasser of Egypt). The book had already been widely published worldwide. Lord Keith held that:

> **[G]eneral publication in this country would not bring about any significant damage to the public interest …. All such secrets as the book may contain have been revealed to any intelligence services whose interests are opposed to that of the United Kingdom.**[31]

6.6.2 Lord Goff's decision is also instructive:

> **[T]he principle of confidentiality only applies to information to the extent that it is confidential …. [O]nce it has entered … the public domain … then, as a general rule, the principle of confidentiality can have no application to it.**[32]

6.6.3 As for European law, in **Verenigung Weekblad Bluf! v Netherlands**,[33] the European Court on Human Rights held that the Netherlands had infringed article 10 (the free speech guarantee) of the European Convention of Human Rights where its courts ordered the withdrawal of an issue of a magazine containing a report on the internal security service dated six years before the issue. The Court held that withdrawal of the magazine could no longer be regarded as necessary to safeguard national security, as the information was already in the public domain.[34] The Court noted that 2,500 copies of the magazine had already been sold in Amsterdam and that the media had commented on the information in the report.

6.6.4 SANEF and PMSA submit that in light of this jurisprudence, the Bill should specifically recognise a public domain defence.

7. Overbroad definitions

National security

7.1 PMSA and SANEF are concerned that despite the important and welcome changes made to limit the definition of "national security", the definition may still be overbroad.

---

[31] At 642. See also Lord Griffiths at 652, who stated that if the injunction had been issued, "**the law would indeed be an ass, for it would seek to deny to our citizens the right to be informed of matters which are freely available throughout the rest of the world**".

[32] At 659.

[33] (1995) 20 EHRR 189.

[34] At 203.

7.2 The definition commences with the following words: "national security includes" (own emphasis). The main problem in this regard is the use of the word "includes" which could be interpreted to mean that the narrowly defined category of matters set out in the definition does not constitute the totality of matters that fall within the concept of national security.

7.3 It is unclear whether the word "includes" was deliberately inserted to indicate that the matters listed in the definition are not exhaustive or whether this was a drafting oversight.

7.4 To the extent that the intention was to broaden the definition beyond what is set out in the Bill, SANEF and PMSA submit that this would render the definition overbroad and unworkable. It would effectively permit a classifying authority to argue that any matter falls within national security.

7.5 We submit that the correct course of action, which appears to have been accepted in principle by the Ad Hoc Committee, is to adopt a narrow definition of national security that does not lend itself to abuse. In order to achieve that objective the word "includes" should be deleted from the definition of national security.

7.6 The definition of national security also includes under sub clause (v) the "exposure of economic, scientific or technological secrets vital to the Republic". SANEF and PMSA are concerned that the inclusion of these matters in the definition renders it overbroad and extends the definition to issues which do not ordinarily fall within the concept of national security.

7.7 Such a provision also has potential for abuse with respect to classifying economic data and could lead to stifling of research into scientific and technological matters.

7.8 Moreover, South Africa is a party to the International Covenant on Civil and Political Rights ("**the ICCPR**") and is bound to uphold the right to freedom of expression, which is guaranteed under article 19 of the ICCPR. Indeed, clause 6(i)(ii) of the Bill specifically states that the measures effected under the Bill must be consistent with article 19 of the ICCPR as well as South Africa's international obligations.

7.9 The Human Rights Committee ("**the HRC**") is the body charged with interpreting and overseeing the implementation of the ICCPR by state parties. In its 2001 concluding observations on Uzbekistan's state report, the HRC noted with concern

that the Uzbekistan Law on Protection of State Secrets included in its definition of "*state secrets and other secrets*" issues relating to science, banking and the commercial sector.[35] The HRC stated that this rendered the restrictions on freedom of expression too wide to be consistent with article 19 and requested that Uzbekistan amend the law to reduce the types of issues defined as state secrets.

7.10 We submit that the HRC's comments are of direct application to the inclusion of economic, scientific and technological matters in the definition of national security.

State security matter

7.11 The definition of "state security matter" is problematic because it also uses the word "includes" and therefore suggests that the definition could be broadened to cover material which is not specified in the Bill.

7.12 PMSA and SANEF submit that the word "includes" should be deleted from this definition as well.

8. Classification of information by members of the security services

8.1 In terms of clause 13(6), every member of the security services as contemplated in chapter 11 of the Constitution has the authority to classify information, subject to confirmation by the head of the organ of state in question.

8.2 The authority given to members of the security services in terms of clause 13(6) vastly extends the number of people that have the authority to classify information. No attempt is made to confine the said authority to members of the security services with a particular rank. Consequently, even the most junior and inexperienced member of the security services will be able to classify information. This flies in the face of the general principle in clause 13(4) of the Bill that information must be classified at a sufficiently senior level to ensure that only information that genuinely requires protection is classified.

8.3 The provision made for the classification decision to be reviewed by the head of the organ of state concerned does not remedy the problems created by clause 13(6) because:

---

[35] Available at http://www.unhchr.ch/tbs/doc.nsf/(Symbol)/CCPR.CO.71.UZB.En?Opendocument (Accessed on 11 October 2011).

8.3.1 Firstly, it is not clear from clause 13(6) how soon the review must take place after the classification decision is made. This could lead to the information remaining classified for an indefinite period of time before a reviewer decides that the information should never have been classified in the first place;

8.3.2 During the time that the information remains classified, regardless of whether it has been correctly classified, all the consequences of classification will follow. This means that the public will be deprived of its right of access to information in respect of that information and all the criminal sanctions in the Bill will also be applicable.

8.4 The potential for abuse in respect of section 13(6) is self evident and we submit that the section must be deleted from the Bill.

9. **Classification of whole document when only part classifiable**

9.1 Having regard to the presumption of openness as reflected in section 32 of the Constitution, the founding values of accountability and openness and the requirement that legislation adopt the least restrictive means possible in terms of section 36(1)(e) of the Constitution, we submit that the Constitution requires that information should only be kept away from the public to the limited extent that it is necessary to achieve specified national security objectives.

9.2 For that reason, the legislation ought to require that where only part of a given document gives rise to security concerns, only that part of the document should be classified. The remainder should be released to the public.

9.3 This appears from **Masetlha** , where Yacoob J expressed this principle as follows:

> **The public is entitled to know all except that which cannot be revealed on account of important national security considerations.**[36]

9.4 The same approach was taken by the majority in **Masetlha** where the Court had to determine whether Independent Newspapers was entitled to access restricted documents in the Court record. The documents in questions were annexures to an affidavit that state security officials had classified as “secret” or “confidential”. In

[36] **Masetlha** at para 103.(minority judgment, but not in respect of this principle).

upholding the objection to the release of a redacted paragraph contained in an annexure, Moseneke DCJ condoned the selective confidentiality restriction,

> **Moreover the confidentiality claim is tailored to a single paragraph and thus its invasiveness has been sharply curtailed.**[37]

9.5 Similarly, in respect of a report attached to an affidavit, Moseneke DCJ upheld the objection by the State on the basis that the report was "*slenderly tailored to conceal only the particularised and sensitive material*."[38]

9.6 This principle is also reflected in section 28 of PAIA, which requires that any information in a record that is not protected and that can reasonably be severed from the protected parts of the record must be severed and disclosed.

9.7 Yet, the Bill contains no such provision. We therefore suggest that a section in similar terms to section 28 of PAIA be included.

10. Categories of classified information

10.1 Clause 13(5) of the Bill provides that once information is classified all information falling under that category is deemed classified. SANEF and PMSA submit that the inclusion of this method of bulk classification will result in the decision maker being absolved from the responsibility to consider and apply their mind to all the specific records which fall within that category.

10.2 This approach to bulk classification is dangerously restrictive of access to information and free speech. The classification of any document that does not have the potential to harm a narrowly defined concept of national security is patently unjustifiable. The mere fact that bulk classification would be expedient or administratively efficient cannot serve as a justification for limitation of fundamental rights.

11. Request for access to classified information and status review

11.1 Clause 19 provides that when a request has been made for access to classified information the request must be referred to the head of the organ of state to review

---

[37] **Masetlha** at para 66.

[38] **Masetlha** at para 73.

the status of the classified information. In accordance with clause 19(3) the information must be declassified and access granted only where there is evidence of a substantial contravention or failure to comply with the law, imminent and serious public safety risk and when public interest outweighs the harm of disclosure.

11.2 SANEF and PMSA are of the view that the circumstances under which information can be declassified when a request for declassification is made are too narrow and amount to an unjustifiable limitation on the right to access information.

11.3 Clause 19 should be amended to state that, in addition to the factors already set out in that section, when a request is made for information to be declassified, the information will be evaluated afresh and if it is found that it does not meet the criteria for classification (and ought never to have been classified in the first place), it will be declassified.

12. **The powers of courts and the open justice principle**

12.1 Clause 52 of the Bill deals with the protection of state information before Courts. It provides that where classified information is placed before a court, such information may not be disclosed to the public unless the court orders such disclosure.[39]

12.2 Before making such an order, the Court is required to take reasonable steps to receive submissions from the party that classified the document or the Director – General of the Agency.[40] This is sensible.

12.3 However, the Court is given a discretion about whether to require information from any other interested party.[41] We submit that this is problematic. Given the well-established open justice principle, where a Court is going to withhold information from the public, it is imperative that all interested parties be afforded the opportunity to be heard.

13. **The offence of accessing a state owned computer**

[39] Clause 52(1)(a)
[40] Clause 52(4)
[41] Clause 52(6)

13.1 The offences created under clauses 40(6) (b) - (d) do not appear to be directly relevant to the Bill and create criminal sanctions in respect of conduct which may be harmless or otherwise lawful.

13.2 In particular, clause 40(6)(b) seeks to impose criminal penalties on any person who gains unauthorised access to a computer which belongs to the state. The subsection does not specify that any harm must result or that the person concerned must have an intention to gain unauthorised access to classified or confidential information or to perform some act which is otherwise unlawful.

13.3 Clauses 40(6)(b) is draconian and could result in a person being convicted for accessing a computer owned by the state even if the intention was to access information which the person was lawfully entitled to receive. This problem is exacerbated by the overbroad definition of "access to a computer", which is contained in clause 40(6)(a). The definition is as follows:

> **"access to a computer" includes access by whatever means to any program or data contained in the random access memory of a computer or stored by any computer on any storage medium, whether such storage medium is physically attached to the computer or not, where such storage medium belongs to or is under the control of the State"**

13.4 This definition is so broad that merely accessing a flash drive owned by the state, regardless of whether it contains classified information, could result in an offence being committed.

13.5 We submit that clause 40(6)(b) should be amended to specify that the computer must be accessed with the intention to access information which the accused was not lawfully entitled to receive.

14. **Conclusion**

14.1 Although the Bill in some respects contains improved provisions compared to its initial draft, in significant and crucial respects, the Bill does not properly calibrate the interests of openness and transparency, and the rights to freedom of speech, and access to information, with national security concerns. The Bill has the potential to play a significant role in transforming our society from a culture of secrecy and repression to one of transparency, accountability and responsiveness, and to become a leading precedent for open and democratic

governments the world over. To achieve these goals and the desirable objectives it articulates, the Bill must properly respect openness, free speech, and access to information, in the various ways that we have suggested.

WEBBER WENTZEL

Ref: Dr Dario Milo/ Ms Okyerebea Ampofo-Anti/ Ms Robyn Muller

Tel: +27 11 530 5232

Fax: +27 11 530 6232

dario.milo@webberwentzel.com

Annexure A

EXECUTIVE SUMMARY

SUBMISSIONS TO THE AD HOC COMMITTEE ON THE PROTECTION OF INFORMATION BILL B6-2010 IN THE NATIONAL ASSEMBLY

SUBMITTED ON BEHALF OF PRINT MEDIA SOUTH AFRICA

1. Introduction

1.1 PMSA submits that aspects of the Protection of Information Bill B 26-2010 ("**the Bill**") are unconstitutional in that they offend the values of openness, accountability and transparency underlying the Constitution, and the constitutional rights to freedom of expression and access to information.

1.2 It is undoubtedly the case that the topics dealt with in the Bill are of great significance to our democracy. Moreover, the drafters of the Bill deserve credit for crafting proposed legislation that is radically different to the apartheid-era Protection of Information Act 84 of 1982 and that in large measure strives to accommodate conflicting constitutional interests and rights of the public and the state, in a balanced and equitable manner.

1.3 There are nevertheless significant aspects of the Bill – issues that go to its heart, such as the tests employed for classifying information, and the offences that are proposed to be created – which in PMSA's submission fail to pass constitutional muster, in respects that will significantly restrict investigative reporting on matters of public interest.

2. The constitutional background

2.1 The values of openness, accountability and transparency are underlying values of the Constitution of the Republic of South Africa 108 of 1996 ("**the Constitution**"). The Constitution also expressly protects the right to freedom of expression and media freedom. It is significant that the guarantee of media freedom is designed to serve the interest that all citizens have in the free flow of information which is possible only if there is a free press.

2.2 The Constitution also protects the right of access to information. The Promotion of Access to Information Act 2 of 2000 ("**PAIA**") was promulgated to give effect to the constitutional right of access to information.

3. National security as a limitation on constitutional rights

3.1 It is trite that no right is absolute. The rights to freedom of expression, and access to information, and the principle of open justice may all yield to more compelling state interests. PMSA accepts that one such compelling state interest that is in principle capable of legitimately restricting the constitutional rights of free speech and access to information, is the protection of national security.

3.2 The point of departure with respect to the Bill is that, although in principle it is legitimate for national security interests to justifiably limit rights, the burden of justification in this context is firmly upon the state. Provisions of the Bill that limit the rights to freedom of expression and access to information, and the principle of open justice, will therefore not survive constitutional scrutiny unless these restrictions comply with section 36 of the Constitution. PMSA submits that in the respects outlined below, this threshold has not been met.

4. The unconstitutionality of aspects of the Bill

4.1 Offences that undermine media freedom

4.1.1 PMSA submits that a number of aspects of the Bill that relate to the criminal offences that have been created in the Bill, are unconstitutional. A number of criminal offences are capable of application to investigative journalists.

4.1.2 These include clause 18 of the Bill which prohibits possession of classified information; clause 32, which creates the espionage offence; clause 33 which creates the hostile activity offence; clause 35 which prohibits accessing of classified information; clause 43 which creates a general 'state security' offence in respect of publication of unclassified information and clause 45 which creates the disclosure offence.

4.1.3 Apart from the severe and, we submit, disproportionate penalties (including the new minimum sentences) that are attached to these

offences, we submit that the main constitutional difficulties that arise from these offences from a media perspective are the following:

4.1.3.1 first, no public interest defence has been proposed. A journalist or editor who is prosecuted under any of the offences cannot argue that the information is of public benefit, e.g. in that it exposes wrongdoing, incompetence, criminality, or hypocrisy. The recognition of such a defence would accord with other aspects of freedom of expression law in analogous contexts, for instance PAIA, the Films and Publications Act of 1996, and our common law of privacy. PMSA submits that the failure to provide for a defence of public interest coupled with the vagaries of the offences created and the severe penalties involved, will create a chilling effect on freedom of expression. This will drastically undermine public discourse, discussion and debate on matters of political speech, which ought to receive heightened protection. It is noteworthy that in the Explanatory Note on the 2008 Bill which was issued by the Ministry of Intelligence on 13 June 2008, it was stated that "**the Minister has no objection to the inclusion of a public interest exemption**". Moreover, foreign jurisprudence and analysis support the introduction of such a defence. ,

4.1.3.2 secondly, PMSA submits that a public domain defence should also be included in the Bill which will be available where the information is already in the public domain. The need for such a defence finds support both in the case law of our domestic courts and court decisions in other jurisdictions.

4.2 **The classification regime**

4.2.1 The Bill envisages that once information is classified, its accessibility to members of the public and its disclosure is limited. The classification of information therefore constitutes a clear limitation on both the rights of access to information and the right to freedom of expression, and amounts to censorship of political speech. We submit that in at least four respects this regime suffers from fatal constitutional flaws. These are discussed in more detail below.

Overbroad definitions

4.2.2 PMSA submits that various definitions that lie at the core of the Bill are so wide as to be utterly unworkable and offensive to the principle of legality, and the rights to free speech and access to information.

4.2.3 The doctrine of legality, which is a foundational principle in our Constitution (section 1(c) of the Constitution), requires that laws must be clear and accessible. The Constitutional Court has endorsed the proposition that laws must be drafted with sufficient precision to allow those who are tasked with their implementation to have reasonable certainty about the conduct that is required of them.

4.2.4 The basic requirement for classification is that information must be "**sensitive**" information. The definition of sensitive information is of particular concern because it links to the concept of "**national interest**", which is defined so broadly as to be, we submit, unconstitutional.

4.2.5 It is submitted that given the breadth of the definition of "national interest" in the Bill, it will be difficult, if not impossible, for government officials charged with the duty of classifying information, to properly ascertain which information ought to be classified. There exists a real danger that such an official would – even if acting in good faith – engage in overclassification. To take two examples of obvious overbreadth, clause 11(1)(a) states that the "**national interest**" includes "**all matters relating to the advancement of the public good**", and clause 11(2)(b) proclaims that the concept also includes "**the pursuit of justice [and] democracy**". Such concepts are so broad as to potentially cover all conceivable aspects of a citizen's existence in our democracy. Rather than dramatically curtailing the definition of "national interest" as proposed in submissions in respect of the 2008 Bill, the definition in fact expands upon that overbroad definition by adding all records that are subject to mandatory protection in terms of sections 34 – 42 of PAIA. This inclusion is patently absurd. PMSA submits that the Bill's extension of the concept of "national interest" in this manner, and indeed the very breadth of the definition itself, betrays an obsession with secrecy that cannot be countenanced in a democracy.

4.2.6 It is submitted that the definition of "security" is also impermissibly broad as "security" is defined as "**to be protected against loss or harm, and is a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts**".

4.2.7 The drafters of the Bill have substantially amended the narrow definition of national security which was contained in the 2008 version of the Bill and which was arguably defensible. The definition of "national security" embraces a wide range of matters which PMSA submits ought not to fall within the compass of national security. The two fundamental problems with the definition of national security are that it includes nebulous concepts and an extremely broad category of issues that could fall within the definition and) the list of more specific matters contained in the definition is not exhaustive.

4.2.8 A further problematic definition is that of a "**State security matter**", disclosure of which triggers a criminal offence. The definition is impermissibly vague and overbroad as it essentially covers every aspect of any matter that relates to the activities of the security services. And, exacerbating this position, the definition covers information which is not necessarily classified and as such may not carry any markings that indicate that it is the type of information that may not be disclosed.

4.2.9 In order not to fall foul of constitutional guarantees and particularly in light of South Africa's repressive history of thought control by the apartheid state, PMSA recommends that the definitions of "national interest", "security" and "state security matter" should be replaced with a single, narrow and defensible definition of "national security matter": The concept must be precisely and narrowly defined such that any impairment on constitutional rights will be justifiable, as is also required under the UN-endorsed Johannesburg Principles on National Security, Freedom of Expression and Access to Information, and in international jurisprudence.

The misplaced protection of commercial information

4.2.10 While it may in principle and in exceptional circumstances be defensible for classification to take place of commercial information pertaining to an organ of state, this protection ought in our submission not to extend to commercial information of private individuals and entities in the possession of the State. Indeed, the Bill even contemplates classification of commercial information of other parties which is not in the hands of the state.

4.2.11 Private individuals and entities are granted sufficient protection in respect of commercial information by PAIA and the common law. It is therefore not only unnecessary to use the moment of the Bill to create an additional layer of protection in this regard, but it is also disproportionate to criminalise the disclosure of such commercial information on pain of severe prison sentences.

4.2.12 It also appears that with respect to classification of commercial information, the Bill is not in line with international practice in that the relevant laws in the United Kingdom, the United States of America (on which the Bill appears to have been modelled) and Canada relating to classification of state information, do not protect and seek to classify commercial information.

Impermissibly speculative levels of classification

4.2.13 The Bill prescribes classification levels that are ostensibly designed to protect information at successive levels of confidentiality. Clause 15 of the Bill prescribes three classification levels, i.e. "Confidential", "Secret" and "Top Secret".

4.2.14 What all the thresholds for classification have in common is the insistence by the drafters that speculative harm will suffice for classification and hence censorship. Thus a document, for instance, will be classified as "**Top Secret**" if its disclosure "**may cause serious or irreparable harm" to "the national interest**"; it will be classified as "**Secret**" if its disclosure "**may endanger" the "security or national interest**"; and it will be classified as "**Confidential**" if its disclosure "**may be harmful**" to the "**security or national interest**".

4.2.15 PMSA submits that the tests for determining the degree of harm that may arise from the disclosure of information is set at an impermissibly low bar for all three classification levels.

4.2.16 The Bill's reliance on such low threshold tests for harm is unconstitutional. Such tests result in widespread over-classification and hence censorship of documents of potential public interest.

4.2.17 In our free speech jurisprudence, and in analogous contexts such as contempt of court, and under PAIA, our courts have clearly required a high degree of harm before imposing liability. The same is true of numerous international jurisdictions. The Bill runs counter to these developments.

4.2.18 A commitment to freedom of expression impels the result, we submit, that records should only be classified if the harm to national security sought to be prevented thereby is at least reasonably likely to occur, substantial and demonstrable

Miscellaneous problems with the classification and declassification regime

4.2.19 *Independent oversight mechanism*

The Bill does not make provision for an independent oversight mechanism to review classification decisions. We submit that in order to guard against the problem of over-classification, an independent and expert oversight body accountable to Parliament should be created to periodically review classified documentation, and to hear appeals from decisions of the heads of organs of state.

4.2.20 *Clauses 7(1), 14(2), 16(5) and 16(6) of the Bill*

These provisions provide for the classification of broad categories and subcategories of information, files, integral file blocks, file series or categories of information, and permits all individual items that fall within such a classified group of documents to be automatically classified.

This approach to bulk classification is dangerously restrictive of access to information and free speech. The classification of any document that

does not have the potential to harm those interests is patently unjustifiable. The mere fact that bulk classification would be expedient or administratively efficient cannot serve as a justification for limitation of fundamental rights.

4.3 **Access to court documents**

4.3.1 Clause 46 of the Bill deals with protection of State information before courts. PMSA submits that clause 46 fails to give proper effect to the principle of open justice which our courts, both in the pre- and post-constitutional era, have emphasised as an essential element of the proper administration of justice.

4.3.2 Clause 46 fails to pass constitutional muster in a number of material respects:

4.3.2.1 first, clause 46(1) of the Bill, which provides that classified information that is placed before a court may not be disclosed to any person not authorised to receive this information unless a Court orders full or limited disclosure, undermines the principle of open justice. The starting point it envisages is that classified information before a court may not be disclosed unless a Court orders disclosure. This is inconsonant with the position adopted in our jurisprudence in regard to a limitation of open justice;

4.3.2.2 secondly, the provisions in clause 46 which compel courts to issue directions for the proper protection of classified information during the course of proceedings, which may include holding proceedings or part thereof *in camera* (clause 46(2)), and also which compel courts to not order classified information to be disclosed without taking reasonable steps to obtain the submissions of the classification authority (clause 46(3)), severely hamstring the ability of courts to regulate their own process, in violation of section 173 of the Constitution;

4.3.2.3 thirdly, PMSA submits that the injunction, contained in clause 46(4), that the hearing in relation to whether documents should be disclosed should always take place *in camera*, and the absolute rule that the submissions as to why the documents should be kept

secret should not be disclosed, in addition to fettering of courts' discretion, constitute drastic interferences with the right to open justice ;

4.3.2.4 fourthly, PMSA submits that clause 46(5) of the Bill, which adopts a blanket prohibition against litigants having sight of classified information, does not accord with the jurisprudence of the Constitutional Court;

4.3.2.5 fifthly, clause 46(9) of the Bill is also unconstitutional. It is objectionable to allow the head of an organ of state to apply to court for an order restricting the disclosure of unclassified State information that is contended to harm the "national interest";

4.3.2.6 finally, clause 46(8), which criminalises the disclosure or publication of any classified information in contravention of an order or direction issued by a court in terms of clause 46 of the Bill, is unnecessary and fails to take into account developed principles of criminal liability. .

4.4 **Other laws that restrict the disclosure of "classified information"**

4.4.1 There are several pieces of national legislation dealing with the confidentiality and classification of State information, such as:

4.4.1.1 section 104(7) and 104(19) of the Defence Act 42 of 2002;

4.4.1.2 section 103(d) of the Intelligence Services Act 65 of 2002; and

4.4.1.3 section 8A and 8B of the National Supplies Procurement Act 89 of 1970.

4.4.2 PMSA is concerned that the Bill does not propose to repeal any of these provisions. As it presently stands, therefore, parallel systems of classification of information will exist, despite clause 17 of the Bill, which provides that the decision to classify information must be based solely on the guidelines and criteria set out in the Bill and the policies and regulations made in terms of the Bill.

4.4.3 Thus, while the Bill will hopefully provide enhanced protection for the media, the classification regimes or powers in existing pieces of legislation will remain restrictive of the rights to access to information and free speech.

5. Conclusion

5.1 We have submitted that the Bill is in many respects a welcome change to the national security landscape in South Africa.

5.2 However, in significant and crucial respects, the Bill does not properly balance the interests of openness and transparency, and the rights to open justice, freedom of speech, and access to information, with national security concerns. Indeed, in its present form, the Bill will result in widespread and unjustifiable censorship, will undermine investigative journalism, and will result in little oversight for classification decisions. These harmful consequences must be avoided at all costs, given the overall significance of the Bill to our constitutional project.

Dr Dario Milo, Okyerebea Ampofo-Anti and Duncan Wild

WEBBER WENTZEL ATTORNEYS

on behalf of Print Media South Africa

25 June 2010

Annexure B

EXECUTIVE SUMMARY

SUBMISSIONS TO THE ANC INFORMATION BILL COMMITTEE REGARDING THE PROTECTION OF INFORMATION BILL B 6B – 2010 ON

SUBMITTED ON BEHALF OF PRINT MEDIA SOUTH AFRICA ("PMSA") AND THE SOUTH AFRICAN NATIONAL EDITORS' FORUM ("SANEF")

1. **Introduction**

1.1 SANEF and PMSA submit that aspects of the Protection of Information Bill B 6B-2010 ("**the Bill**") are unconstitutional in that they offend the values of openness, accountability and transparency underlying the Constitution, and the constitutional rights to freedom of expression and access to information.

1.2 It is undoubtedly the case that the topics dealt with in the Bill are of great significance to our democracy. The drafters of the Bill deserve credit for crafting proposed legislation that is different to the apartheid-era Protection of Information Act 84 of 1982.

2. **The constitutional background**

2.1 The values of openness, accountability and transparency are underlying values of the Constitution of the Republic of South Africa 108 of 1996 ("**the Constitution**").

2.2 The importance of freedom of expression to an open and democratic society, and particularly the role of the media in a democracy, has been reiterated by our highest courts on numerous occasions. It is significant that the guarantee of media freedom is designed to serve the interest that all citizens have in the free flow of information which is possible only if there is a free press.

2.3 The Constitution also protects the right of access to information in section 32. The Promotion of Access to Information Act 2 of 2000 ("**PAIA**") was promulgated to give effect to the constitutional right of access to information.

2.4 It is trite that no right is absolute. The rights to freedom of expression, and access to information may yield to more compelling state interests. PMSA

and SANEF accept that one such compelling state interest is the protection of national security. It is legitimate for national security interests to justifiably limit rights but the burden of justification in this context is firmly upon the state. Provisions of the Bill that limit the rights to freedom of expression and access to information will therefore not survive constitutional scrutiny unless these restrictions comply with section 36 of the Constitution.

3. **Criminal offences that undermine media freedom**

3.1 SANEF and PMSA submit that a number of the criminal offences set out in the Bill are unconstitutional in that they disproportionately limit the right of access to information and freedom of expression (including media freedom). These offences include:

3.1.1 clause 36 of the Bill which creates the espionage offence;

3.1.2 clause 37 which creates the offence of receiving state information;

3.1.3 clause 38, which creates the hostile activity offence;

3.1.4 clause 40(1), which makes it an offence to intentionally access classified information;

3.1.5 clause 43, which creates the offence of disclosing classified information;

3.1.6 clause 44, which makes it an offence to fail to comply with clause 15. Clause 15 in turn requires each person to return any classified information in their possession to the South African Police Service; and

3.1.7 Clause 49, which makes it an offence to disclose a “state security matter”.

3.2 SANEF and PMSA submit that the main constitutional difficulties that arise from these offences from a media perspective are the following:

3.2.1 The offences created in clauses, 36, 37, 38 and 39 are inconsistent with the common law principle that conduct is not unlawful unless committed with a guilty mind. The effect of the words "knows or ought reasonably to know", which are used in each of these clauses, is that each of these offences can be committed even if the accused does not

have actual knowledge. The Bill should require that the accused needs to have committed the crime with knowledge of its illegality, including that he or she was disclosing classified information, and with the intention to cause substantial harm to national security.

3.2.2 The Bill does not provide for an explicit public interest defence. SANEF and PMSA submit that the case for a public interest defence is overwhelming. Such a defence would allow a whistleblower or journalist who publishes classified information to argue that the disclosure was justified, for instance because it revealed evidence of significant incompetence, criminality, wrongdoing, abuse of authority or hypocrisy on the part of government officials. The failure to provide for a defence of public interest coupled with the vagaries of the offences created and the severe penalties involved will undoubtedly create an unjustifiable chilling effect on freedom of expression.

3.2.3 The Bill should also be amended to include a public domain defence. This defence postulates that where the information is already in the public domain, future restrictions on its publication would be futile. We submit that it would not be correct to argue that harm to national security would likely ensue from the republication of information that is already in the public domain.

3.2.4 A number of the criminal offences clauses in the Bill fail to recognise the maxim *ne bis in idem* which provides that no person can be tried for the same offence twice. This is recognised in the section 35(3) of the Constitution and section 106(1)(c) of the Criminal Procedure Act 51 of 1997. The offences created in clause 49 (disclosure of state security matter) and clause 43 (the general disclosure offence) overlap and therefore when a person commits an offence such person will also commit an offence under clause 43. Furthermore, if one has regard to the offences created in clauses 49(c), 44 and 37, a person could be subject to three separate sentences if they are in possession of information that relates to a 'state security matter'.

4. **Overbroad definitions**

National security and State Security Matter

4.1 PMSA and SANEF submit that the definition of "national security" and "state "security matter" may still be overbroad. The main problem in regard to the definitions is the use of the word "includes". It is unclear whether the word "includes" was deliberately inserted to indicate that the matters listed in the definition are not exhaustive or whether this was a drafting oversight. SANEF and PMSA submit that this use of the word “includes” renders the above definitions overbroad and unworkable and consequently it should be deleted from both definitions.

5. **Classification of information by members of the security services**

5.1 Clause 13(6) empowers every member of the security services as contemplated in chapter 11 of the Constitution to classify information, subject to confirmation by the head of the organ of state in question. No attempt is made to confine the said authority to classify information to members of the security services with a particular rank. This flies in the face of the general principle in clause 13(4) of the Bill that information must be classified at a sufficiently senior level.

5.2 The review of classified information by the head of the organ of state concerned does not remedy the problems created by clause 13(6) because it is not clear how soon the review must take place after the classification decision is made.

5.3 Section 13(6) carries potential for abuse and we submit that the section must be deleted from the Bill.

6. **Categories of classified information**

6.1 The accessibility of information to members of the public and disclosure of information is drastically limited once the information is classified. SANEF and PMSA submit that the inclusion of the method of bulk classification provided in clause 13(5) will result in the decision maker being absolved from the responsibility to consider and apply their mind to all the specific records which fall within that category and is dangerously restrictive of access to information and free speech.

7. **Request for access to classified information and status review**

7.1 SANEF and PMSA are of the view that the circumstances under which information can be declassified under clause 19(3) are too narrow and amount to an unjustifiable limitation on the right to access information. Clause 19(3) should be amended to state that, in addition to the factors already set out in that clause, when a request is made for information to be declassified, the information will be evaluated afresh and if it is found that it does not meet the criteria for classification (and ought never to have been classified in the first place), it will be declassified.

8. **The offence of accessing a state owned computer**

8.1 The offences created under clauses 40(6) (b) - (d) do not appear to be directly relevant to the Bill and create criminal sanctions in respect of conduct which may be harmless or otherwise lawful. The definition of "access to a computer" is so broad that merely accessing a flash drive owned by the state, regardless of whether it contains classified information, could result in an offence being committed. We submit that clause 40(6)(b) should be amended to specify that the computer must be accessed with the intention to access information which the accused was not lawfully entitled to receive.

9. **Conclusion**

9.1 We submit that the Bill is in many respects a welcome change to the national security landscape in South Africa. The Bill has the potential to play a significant role in transforming our society from a culture of secrecy and repression to one of transparency, accountability and responsiveness, and to become a leading precedent for open and democratic governments the world over. To achieve these goals and the desirable objectives it articulates, the Bill must properly respect openness, free speech, and access to information, in the various ways that we have suggested.

WEBBER WENTZEL on behalf of Print Media SA and SANEF

28 October 2011