

BREAKING THE LOGJAM?

AN ASSESSMENT OF “EVALUATING THE INFORMATION BILLS: A BRIEFING PAPER ON THE PROTECTION OF INFORMATION BILL” PREPARED BY IAIN CURRIE AND JONATHAN KLAAREN ON BEHALF OF THE CENTRE FOR MEMORY AT THE NELSON MANDELA FOUNDATION, JUNE 17, 2011

Stefaans Brümmer, M&G Centre for Investigative Journalism

June 22, 2011

ABOUT THIS ASSESSMENT

1. This assessment is intended to assist the Right2Know Campaign (R2K) and others in civil society concerned about the Protection of Information Bill (the Bill) to formulate a position vis-a-vis efforts by the Nelson Mandela Foundation (NMF) to mediate the apparently intractable differences between the Ministry of State Security and opponents of the Bill.
2. In particular, the assessment seeks to guide decision making on whether the proposal, implicit in Currie and Klaaren’s paper, to break the logjam by splitting the Bill into two – one a classical “official secrets law” and the other a “government information security law” – should be supported.¹
3. The assessment has been prepared in haste and should not be regarded as a comprehensive response.
4. The assessment has been prepared for the M&G Centre for Investigative Journalism (MGCIJ or amaBhungane), a non-profit centre founded to develop investigative journalism in the public interest. Our mandate includes engaging in advocacy to “defend and expand the democratic space investigative journalists need to do their work”.²
5. MGCIJ and, before its founding its managing partners, the author and Sam Sole, have been active participants in the debate on the 2008 and 2010 versions of the Bill. MGCIJ and the managing partners’ activities have included representations to the 2008 drafting

¹ See e.g. para 30.2 of Currie and Klaaren, where they state: “While this briefing paper cannot give final answers or even a detailed analysis, we [pose] three questions about the fundamental reorientation that the Bill has undergone since its original drafting: from a government information security law to an official secrets law. First, is it possible to sever the parts of the current draft Bill that serve the purpose of an information security law from the parts of the current draft Bill that serve the purpose of an official secrets law? Second, would the purpose of an information security law be better served not as part of an official secrets law but rather as an extension to the PAIA or even as a separate piece of legislation? Third, would the purpose of an official secrets law be better served without the statutorily joint pursuit of the purpose of a governmental information security law?”

² For more on the M&G Centre for Investigative Journalism, see www.amabhungane.co.za.

team, submissions to Parliament's ad-hoc committees processing the 2008 and 2010 versions of the Bill, and an active involvement in R2K.

6. It should be noted that while MGCIJ's mandate is limited to the profession of investigative journalism, our concerns about the effect of the Bill are not. We believe that the Bill as currently drafted represents a fundamental challenge to the open and accountable democracy that the Constitution envisages, with severe consequences not only for journalists but for all South Africans.

PRELIMINARY REMARKS

7. The NMF initiative should be welcomed, as should be the readiness of Ministry of State Security officials and civil society actors to participate in it. And regardless of any criticism of aspects of Currie and Klaaren's paper, it too should be welcomed as a highly lucid and well-informed contribution to the debate.
8. Currie and Klaaren argue convincingly that the motivation for the Bill's drafting was not that of a securocratic or paranoid state, but to replace apartheid-era law with constitutionally compliant law. One should temper this with the addage that the road to hell is paved with good intentions and an appreciation of the fact that the legislative drafting process is contested terrain where different actors with different motives attempt to get their way. Nevertheless, Currie and Klaaren's insights are useful as they may help to deescalate distrust and introduce more rationality into the debate.
9. This assessment will use the following shorthand:
 - 9.1. **Official secrets law:** the same meaning as in Currie and Klaaren, i.e. legislation that aims to prevent the disclosure of state secrets so as to safeguard national security.
 - 9.2. **Government information security law:** the same meaning as in Currie and Klaaren, i.e. legislation that aims to regulate the secure processing of the entire spectrum of valuable and sensitive government information to prevent its inappropriate destruction, loss, alteration or disclosure.
 - 9.3. **A big stick approach:** criminalisation, with *serious penalties* applied to *any person* found guilty of a breach. We argue that a big stick approach is inappropriate for enforcing government information security laws and that even an official secrets law should be enforced with a big stick only if appropriate escape valves consistent with an open and accountable democracy are built in.
 - 9.4. **Escape valves:** mechanisms to ensure whistleblowing and the unauthorised dissemination of information do not attract criminal consequences where the public interest in disclosure overrides what on the face of it would be the state's interest in non-disclosure.
 - 9.5. **Departmental protection:** The protection of state information against unauthorised destruction, loss, alteration or disclosure through disciplinary rather than criminal sanction of state employees (and in any case not ordinary members of the public).
10. This assessment concludes – cautiously – that the splitting of the Bill into an official secrets law and an information security law *may be regarded as a mechanism to break the logjam*, provided that the former does not wield the big stick without appropriate escape valves, and that the latter relies on departmental protection rather than criminal sanction to achieve its aims.

OF GOOD INTENTIONS AND INCOMPATIBLE AIMS

11. Currie and Klaaren trace the introduction of the 2008 version of the Bill to the desire to repeal the unconstitutional Protection of Information Act 84 of 1982 and replace it (together with the problematic Minimum Information Security Standards cabinet policy) with constitutionally compliant legislation.³
12. As drafted, they observe, the 2008 version was “intended to put into law a government duty to process important information in a secure manner that went far beyond the conventionally narrow protection of national security information. In this sense, the Bill was understood as a statutory mirror of the PAIA [Promotion of Access to Information Act], imposing general duties on government to secure information that was identified by the PAIA as meriting protection against disclosure”. But they observe that while PAIA “only stipulates rules for information processing by government *after receipt of a request* made in terms of the Act”, the Bill was intended to provide general rules (i.e. at the outset) for the “proper treatment and non-disclosure of important ... government information”, subject of course to its disclosure where indicated by PAIA.⁴
13. Also stirred into the Bill’s mix was the additional desire to introduce statutory anti-espionage provisions to substitute the “weak regime of common-law criminalisation” derived in part from apartheid-era jurisprudence.⁵
14. The reaction to the 2008 version of the Bill, Currie and Klaaren say, was one of “yes ... but”, with media and freedom of expression advocates criticising the absence of a public-interest defence and the “vague and wide criteria mandating classification”. Before that version of the Bill was withdrawn from Parliament towards the end of 2008, the Ministry of Intelligence (as it was then called) mooted the inclusion of a public interest defence.⁶
15. When the Bill was reintroduced in 2010, the muted reaction was replaced by “a level of public concern and outrage that no other legislative development had merited since the democratic transition”.⁷
16. The principal concern, according to Currie and Klaaren, was the broad scope of the Bill. They continue: “The Bill was certainly broad in scope, particularly if compared to official secrets laws in other jurisdictions. But as we have seen, its scope was principally a product of its legislative history and its intention not only to provide for the protection of state secrets in the narrow sense but also to provide for a comprehensive regime of government confidentiality that would replace the existing regime”.⁸
17. Where things went wrong, they say, is that “the ambitions of the Bill were difficult to reconcile with its provenance in the intelligence ministry and with its overall categorisation as state security legislation, providing as it did for a classification regime and for the prohibition of offences such as espionage and sabotage. Put another way, an official secrets law seemed a disconcertingly odd place to find provisions relating to the

³ Currie and Klaaren, para 12-15.

⁴ Op cit, para 16

⁵ Op cit, para 18

⁶ Op cit, para 19-20

⁷ Op cit, para 23

⁸ Op cit, para 25

secure treatment of valuable information and general prohibitions on disclosure of sensitive information.”⁹

18. Following initial resistance, the Minister of State Security proposed amendments, leading to the current working draft. This draft, Currie and Klaaren argue, “no longer serves the broad purpose of regulating the secure processing of valuable state information. It is now more narrowly official secrets legislation in the conventional sense”.¹⁰
19. However, they agree, “the scope of the Bill remains extremely broad, purporting to regulate all state information..., allowing classification at a non-secret level of ‘confidential’ ... and applying ... to all organs of state... This may reflect a continuing desire to have a law that regulates confidentiality of state information – that the Bill is an information security law rather than merely an official secrets law.”¹¹

Comment

20. Reading Currie and Klaaren’s account of the Bill’s origin and subsequent permutations is like watching a train crash in slow motion. They convincingly ascribe the sorry state of the current working draft of the Bill to the evolving confusion between two types of legislation:
 - 20.1. official secrets law, which should concern itself only with state secrets that truly need to be protected to safeguard the nation’s security; and
 - 20.2. government information security law, which should concern itself with the proper and secure treatment of government records so that they are not shredded when they should be preserved for government’s proper functioning or posterity, left behind on trains and buses, or handed out willy-nilly to third parties without considering whether disclosure would undermine a legitimate government or third-party interest.
21. We agree that the muddling of these contending aims contributed to some of the worst features of the current working draft of the Bill. These include:
 - 21.1. Its very broad scope, which would potentially enable not just state entities handling true state secrets but even the kwaZulu Natal Sharks Board to “protect” information as “top secret” rather than just implementing prudent record management practices; and
 - 21.2. The inappropriate application of the big stick, which would be wielded against any member of the public should they dare handle one of these sharky “secrets”. It is not without reason that R2K has warned that the Bill will create a “society of secrets”.
22. This analysis lends itself to a decision to support a proposal to split the Bill in two – at the very least it will help clarify the divergent aims that are sought to be achieved and help ensure that these divergent aims are not achieved through the same (sometimes grossly inappropriate) enforcement mechanisms.
23. However, before we jump to conclusions a more pointed look at Currie and Klaaren’s analysis may be in order. Some issues:

⁹ Ibid

¹⁰ Op cit, para 29.3

¹¹ Op cit, para 30.1

- 23.1. Currie and Klaaren appear to accept uncritically the grand scheme that underpinned the 2008 version of the Bill, to wit the putative need for a very comprehensive government information security law that would regulate the processing of all government records. While such a law appears academically elegant, there are also some real-world caveats.
- 23.2. The government information security law Currie and Klaaren seem to have in mind implies the need for government officials to make decisions about how to categorise records *when they are produced or come into government's possession*, rather than only when and if a decision needs to be made about e.g. the continued preservation or sharing of a record.
- 23.3. The question is whether such pre-categorisation will not overburden an already stretched bureaucracy; alternatively result in rote decisions skewed towards caution (and hence overprotection).
- 23.4. If indeed the experience is that officials are careless about record storage, preservation and disclosure, a few simple state-wide rules enforced through departmental protection (i.e. where officials are departmentally disciplined rather than officials and outsiders alike criminally prosecuted) may be much more appropriate. Rather than an up-front classification into various categories of all government records, the aim would be to limit upfront decision-making to, e.g. a simple: "This is an important document, it must be preserved as prescribed and not be shared with outsiders without us applying our minds". The initial decision-making will be more limited and when -- and if -- more complex decisions need to be made in selected cases, these will be more likely to be context-appropriate.
- 23.5. Currie and Klaaren's apparently uncritical acceptance of this grand scheme leads them in turn to skirt over some of the more serious problems which emerged already in 2008, and in any case prior to the current working draft.
- 23.6. Major problems in 2008 included the big stick criminalisation across society of simple possession and disclosure even of records that might need protecting but do not contain state secrets in the true sense of the word; and criminalisation in some instances even where records are not formally classified. The latter would of course introduce intolerable uncertainties into any enforcement regime and both of these, again, could only encourage the evolution of a "society of secrets".
- 23.7. Possibly the high-water mark of the grand scheme's adverse manifestations was the academically elegant but bizarre attempt, which was made overt in the initial 2010 version, to make the Bill contiguous with PAIA -- i.e. to slap serious criminal sanctions on the unauthorised possession or disclosure of any information (classified or not and in physical form or not) which is subject to mandatory protection under PAIA.¹² It is worth remembering that mandatory PAIA refusals attach to matters such as a third party's commercial information. Theoretically, a state official blurting out a bidder's pricing in a state tender, and a member of the public who proliferated the information in casual conversation, could both have been jailed for three to five years.

¹² This offence was circumscribed in clause 38 through its reference to clause 11(3)g of the 2010 Bill. It appears to have been deleted in the current working draft.

24. Currie and Klaaren appear to remain proponents of a *comprehensive* government information security law, although now to be split from what would remain as a much tighter and narrower official secrets law. But given the apparent blind spot for the adverse consequences that the grand scheme approach to a government information security law could have, R2K and others in civil society may want to consider seeking common ground regarding the approach to such law this time around before we lend our support to the mooted split.
25. Our recommendations, below, will make more detailed proposals.

FURTHER AREAS OF CONCERN

26. Currie and Klaaren discuss what they consider to be the “principal remaining areas of concern”, in the course of which they give valuable insights and propose a compromise to break the logjam around the demand for a public interest defence.¹³ They identify the following main areas of concern:

- 26.1. Regarding **scope of application** they argue, as already described above, that the discordance between the two approaches led to what they call the “extremely broad” scope even of the current working draft even though it has moved closer to classic official secrets law. This underpins their implied proposal for the Bill to be split.¹⁴
- 26.2. We agree with the analysis.
- 26.3. Regarding the demand for a **public interest defence** they note that as the Bill as drafted is subject to PAIA, the latter’s built-in public interest override will also apply – meaning that if under PAIA a record needs to be disclosed because of an overriding public interest, even a classified record will have to be declassified and disclosed following a PAIA application. But they also note that the PAIA public interest override is burdened by an “unreasonably high threshold” which limits its utility.¹⁵
- 26.4. We agree with this analysis, but would add another serious caveat: To apply under PAIA for a record that one has not seen (or that one cannot admit to having seen because that will unleash a serious criminal investigation into the leak) in sufficient detail to make a convincing case that the record contains information that would mandate its release in the public interest will, in most cases, be a non-starter. And even if that case can be made, PAIA’s built-in bureaucratic delays would often mean that the imminent danger that justified disclosure in the public interest is long gone by the time the record is disclosed.
- 26.5. A much more likely scenario will be of an internal whistleblower bringing a record to an outsider (an NGO worker, union official, MP or journalist), and the latter having to decide whether to return the record immediately and avoid prosecution, or risk prosecution and disclosing the record because he/she firmly believes that it is the right thing to do. In this scenario PAIA’s public interest override will give no succour.

¹³ Op cit, para 30

¹⁴ Op cit, para 30.1-30.2

¹⁵ Op cit, para 30.3

- 26.6. Currie and Klaaren suggest a further, implied, “public interest defence” as a compromise to break the logjam.¹⁶ They say that while in the current working draft criminalisation attaches to the pure fact of whether a record has been classified, the 2008 draft’s approach was “to criminalise the harm caused by disclosure of classified information rather than the fact that classified information had been disclosed”.¹⁷
- 26.7. They argue that a return to the 2008 drafting in this regard would provide an implicit (yet less controversial) public interest defence, as “the use of this substantive drafting style would allow accused persons to argue and attempt to demonstrate that they have in fact acted in a manner that protected rather than harmed the security of the state”.¹⁸
- 26.8. We see no major problem with a compromise along these lines: after all, the demand for a public interest defence has not been for an exemption from prosecution as soon as a public interest is claimed, but rather for a sporting chance to claim in court that the public good sought through disclosure outweighed the public good the state sought through the protection from disclosure.
- 26.9. However, there is one serious caveat: To the best of our understanding the 2008 Bill did not, as Currie and Klaaren state, simply “criminalise the harm caused by disclosure of *classified information*” (our emphasis). The 2008 Bill went well beyond that: it criminalised the harm caused by the disclosure of information, even if the information was not formally classified, if it *matched* the definition of information that could be classified. This was a glaring problem as it would, once again, have introduced an intolerable level of uncertainty, encouraging the evolution of a “society of secrets”.
- 26.10. Consequently, R2K and others in civil society may want to consider lending their support to Currie and Klaaren’s mooted compromise only if there is clear agreement that the 2008 formulation will not be reimported complete with its criminalisation attaching to unclassified information. The solution, we would argue, is to insist that a new formulation should apply criminal consequences only where both conditions apply: the information was classified *and* there was harm.
- 26.11. Regarding **proportionality of penalties**, Currie and Klaaren note that the Bill imposes “very stiff maximum penalties” and since 2010 sets minimum penalties. This compounds the lack of a public interest defence.¹⁹ We concur, but would add that the penalties, and the reduction of a court’s discretion, appear to be inconsistent with South Africa’s human rights culture and aggravate the existing problems of a big stick being wielded to achieve some aims that are far removed from protecting true state secrets.
- 26.12. Regarding an **independent appeals mechanism** and **harmonisation with PAIA**, Currie and Klaaren note that the 2008 drafters did, after representations, moot “an independent oversight and appellate body within the security establishment”, and that “recent press reports suggest that the government will

¹⁶ Op cit, para 30.4-30.8

¹⁷ Op cit, para 30.6

¹⁸ Op cit, para 30.7

¹⁹ Op cit, para 30.9

consider putting into place” an independent mechanism. They also point out that clause 25 of the current Bill provides for PAIA appeals to each department’s minister, following which an appeal to the High Court is possible. They argue that the retention of PAIA-compatibility is crucial to the Bill’s constitutionality, as without it the constitutional right to access information will be infringed.²⁰

26.13. Their insistence on PAIA compatibility is strongly endorsed, but one should note that R2K’s demand that “an independent body appointed by Parliament, and not the Minister of State Security, should be able to review decisions about what may be made secret” is not so much a concern with the minutiae of who will adjudicate appeals when there are individual requests for declassification as with the Minister of State Security’s wide power under the Bill to prescribe to other departments what should be classified and oversee compliance. R2K feels that it is inappropriate for the minister whose department is in the business of secrecy to have this role.

26.14. It appears that the recently mooted mechanism Currie and Klaaren refer to – which apparently will be called a “classification review panel” – is an attempt to address the kind of concern expressed by R2K, but the limited information so far available suggests that the panel will still have to work in important respects with the minister’s concurrence and that it will report findings to Parliament’s generally-closed Joint Standing Committee on Intelligence. It is also not clear how it will be appointed. This means that until and unless there are firm guarantees of the panel’s independence and that it will take over all of the minister’s powers to prescribe to and oversee other departments, R2K’s demand should be regarded as unmet.

26.15. Regarding **accountability of the intelligence agencies**, Currie and Klaaren note the core R2K demand that the Bill must not “exempt the intelligence agencies from public scrutiny”. They then go on to claim that “there is nothing in the current draft of the Bill that would have the effect of exempting organs of state implementing the Bill from public scrutiny ...”²¹

26.16. Their comment appears to be based on a misunderstanding of the R2K demand, possibly occasioned by an imprecise formulation by R2K of its concern with what is one of the Bill’s most draconian (and as of yet unaddressed) weaknesses. The R2K demand refers to clause 43 of the current draft, which criminalises the disclosure, publication, retention, or improper care of information which one “knows or reasonably should know is a state security matter”. A state security matter is extremely widely defined as “any matter which is dealt with by the [State Security] Agency or which relates to the functions of the Agency or to the relationship existing between any person and the Agency”. The penalty is five to 15 years.

26.17. The problems with clause 43 include:

26.17.1. It does not require information to be formally classified – rather no more is required than that the perpetrator “should reasonably know” the

²⁰ Op cit, para 30.10-30.13

²¹ Op cit, para 30.14

information somehow falls into this amorphous concept of a “state security matter”. The old problem of uncertainty rears its head;

26.17.2. It does not require information to be in material form. Even talk can be criminalised; and

26.17.3. The very wide definition of “state security matter” can lead to absurdities such as that when the State Security Agency decides to investigate, for argument’s sake, whether a prolonged drought is a threat to national security, discussion about the drought could be deemed off-limits to the rest of society because it is now a matter “which is dealt with by the Agency”. And in any case, the wide definition *will* quite conceivably allow the agency to avoid scrutiny, as it will outlaw any disclosure “which relates to the functions of the Agency”.

26.18. Clearly R2K’s demand not to limit scrutiny of the intelligence agencies remains unmet.

RECOMMENDATIONS

27. We cautiously endorse a conclusion that the splitting of the Bill into an official secrets law and an information security law *may be regarded as a mechanism to break the logjam*, provided that R2K and others in civil society seek common ground with the promoters of such an idea in a number of areas. We recommend:

In relation to an official secrets law

28. For the splitting exercise to be worthwhile, the resulting rump official secrets law will have to be lean and narrow in scope, and its use of the big stick will have to be tempered with escape valves compatible with an open and accountable democracy. Consistent with R2K demands, it should:

28.1. Limit secrecy to key state departments that deal in matters of national security. These might be the departments of state security, defence, police, and international relations and cooperation. An opt-in clause (with parliamentary approval) could include further state entities in whole or in part, such as those that deal with nuclear proliferation secrets;

28.2. Limit secrecy to matters truly relating to the national security and no more;

28.3. Ideally punish only those responsible for keeping secrets (usually serving and former state officials or contractors) and not society at large;

28.4. Have escape valves in the form of full PAIA compatibility, full Protected Disclosures Act (PDA) compatibility and at least a de facto public interest defence;

28.5. Give a truly independent oversight body, rather than the Minister of State Security, the role of prescribing classification standards for other departments and overseeing compliance;

28.6. Not veil the State Security Agency and its activities in secrecy as in the present clause 43; and

28.7. Punish only where information has been formally classified.

In relation to the mooted public interest defence compromise

29. The proposed solution, of a harms test being satisfied before criminal sanction can apply, has some merit as it will, in a perhaps less controversial way, introduce the same balancing act as a public interest defence – to whet an assessment whether the public good sought through unauthorised disclosure outweighed the public good sought through the protection from disclosure. However, it is recommended that the following safeguard is agreed on:
- 29.1. The harms test will be *in addition to* rather than instead of or as an alternative to classification as was the case in the 2008 Bill. (If this is not ensured, the Bill will introduce an intolerable level of uncertainty about what may or may not be disclosed, encouraging the evolution of a “society of secrets”.)
30. We draw attention to another alternative remedy already implicit in the R2K demands: If it is accepted that criminal sanction should apply only to those responsible for keeping secrets and not to society at large, the need for a public interest defence falls away – provided of course that officials and former officials will have an escape valve – e.g. the Protected Disclosures Act. This is not a far-fetched proposition: the relatively strict US official secrets regime does not prosecute beyond persons with an original duty to keep secrets and their accomplices – the jurisprudence holds that to do so would contravene the First Amendment.

In relation to a government information security law

31. The temptation may be to buy now and worry about the price later – i.e. to take up the offer of a narrowed-down rump official secrets law and postpone concerns about the future shape of a government information security law. However, it is recommended that common ground be sought on the following features of any new government information security law before the split is endorsed:
- 31.1. It should be enforced through departmental protection measures, meaning persons charged with their safekeeping could be disciplined (including dismissal) for contraventions. Criminal sanctions will not apply – and certainly not to ordinary members of the public;
- 31.2. The safety valves of PAIA and the Protected Disclosures Act should apply; and
- 31.3. It should aim to put into place a simple mechanism to determine which government records are valuable/sensitive and therefore deserving of proper safeguarding against destruction, loss or alteration as well as of proper consideration should there be a request for it to be disclosed. Ideally it will not create a complex and burdensome pre-classification system of all government records.