5 April 2018

Dear Dr Motshekga

I write to you on behalf of a group of organisations who were part of the public submissions on the Cybercrimes Bill, who are signatories to the letter as indicated below.

We have reconsidered the Bill at a recent meeting of those organisations on the 3rd April 2018. We have taken into account the analysis of submissions by the Department of Justice, as well as their further submissions to the Police Portfolio Committee in Parliament and meetings of the Justice and Constitutional Development on the Bill.

We remain very concerned that the bulk of the concerns we raised have not been dealt with. We list as Annexure A the some key concerns we still have, although as individual organisations we also have other submissions that have not been dealt with. These speak to very fundamental drafting concerns.

We note that while this is still the 5th Parliament, there have been significant changes in the leadership in the majority party. The previous President did indeed commit to this legislation being tabled, which was done. We would like to put forward for consideration the submission that the Bill may have been tabled before it was in fact ready for tabling. While we have every confidence in the Committee’s processing of the Bill, the range of problems that have been raised are broad and may not be susceptible to Parliamentary amendment.

Under the circumstances, we propose that the Bill be withdrawn from Parliament, and a significant redrafting process be engaged in. In the alternative, we propose an engagement by the experts who made submissions to Parliament, with the DOJ.

Yours faithfully

Alison Tilley

Murray Hunter, Right2Know Campaign.

Mark Heyink, Information Governance Consultancy

Peter Hill, IT Governance

John Giles and Lisa Emma-Iwuoha, Michalsons Attorneys

Jason Jordaan, DFIR Labs Pty Ltd

Gaps and overlaps in overall framework of the Bill. 0

Legal concerns 1

State Security and its role in cybercrime. 3

Technical issues 4

# Gaps and overlaps in overall framework of the Bill.

1. Gap: Minimum Information Security Standards (MISS)

The relationship between this legislation and the Minimum Information Security Standards (MISS) was not addressed, **and remains unaddressed**. The draft Bill and tabled version fail to reference these in any way leave a concerning lacuna as to how the MISS and this legislation cohere.

2. Overlap: Protection of Personal Information Act (POPI) and the right to informational privacy

We also noted that the Protection of Personal Information Act (POPI) and the right to informational privacy was **not adequately considered** in relation to this legislation.

3. Overlap: Protection of State Information Act

There is an overlap with section 38 of the Protection of State Information Act. These issues are dealt with in a different form in section 4 and 7 of this Bill, in so far as state information is concerned. Again, the rationale behind this duplication is unclear.

4. Overlap: The Promotion of Equality and Prevention of Unfair discrimination Act (PEPUDA), and the Riotous Assemblies Act 17 of 1956.[[1]](#footnote-1)

Another overlap in the Bill is The Promotion of Equality and Prevention of Unfair discrimination Act (PEPUDA) which was duplicated in section 17 (Prohibition on dissemination of data message which advocates, promotes or incites hate, discrimination or violence)and section 18 (Prohibition on incitement to violence and damage to property)

Equally, there is also a crime which is incitement to commit a crime, including violence. Incitement to commit any crime is punishable by virtue of the provisions of section 18(2) of the Riotous Assemblies Act 17 of 1956[[2]](#footnote-2).

5. Overlap: Hate crimes and fake news

The offence of speech which is harmful or incites harm may be treated as the subject of a number of criminal charges. Is this section consistent with the constitution? Not in our view.

This issue is also dealt with in the draft Hate Crimes Bill[[3]](#footnote-3)

6. Overlap: The Intimidation Act No 72 of 1982

The Intimidation Act No 72 of 1982 also remains in force.

7. Overlap: Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA)

The Bill also duplicates section 49 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act[[4]](#footnote-4) (RICA).

# Legal concerns

1. Reversal of onus.

The possession offences outlined in Chapter 2 propose a framework whereby the possession of information or software is guilty, unless they can give an ‘exculpatory account’ of the possession.

The presumption falls into the class of “reverse onus” provisions, which are now settled in law as requiring scrutiny, although we concede they are not inevitably unconstitutional.

2. The construction of the offences using the word “unlawful”

One of most important part of the Cybercrimes Bill is the section dealing with creating the most central cybercrime, that of hacking, in section 2. It currently says the access must be unlawful. It doesn't say what unlawfully means. It clearly must mean “when the access is unauthorised”, but it says ‘unlawful’ instead. Unlawful is not just illegal access. Usually we use the word unlawful in relation to the state, where that state does things that are not authorized by law. The state, unlike individuals, must have a law to allow it to act. If the state acts without a law, or in contravention of a law that is unlawful. Normally a criminal provision describes the actual crime, which here is accessing a computer without permission.

As a result the Bill criminalises those persons who process personal information where access is not authorised by law.

3 . Specific concerns: definitions of common law crimes as cybercrimes.

Clauses 11, 12, 13 and 14 in the draft Bill appeared to advance the proposition that a cyber crime is a common law crime, committed with a computer. This is not consonant with the Budapest Convention on Cybercrime[[5]](#footnote-5) (to which South Africa is a signatory but which has not been ratified), which requires parties to

establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

The criminal offence is the changing of the data. It is not the fraud, committed by computer. This is correctly identified in the National Cybersecurity Policy Framework[[6]](#footnote-6) document as **not** cybercrime. The policy document says

However, cybercrime comprises also offences committed by means of

computer data and systems, ranging from the sexual exploitation of children to fraud, hate speech, intellectual property rights (IPR) infringements and many other offences.

Furthermore, any crime may involve electronic evidence in one way or the other. **While this may not be labelled “cybercrime”,** a cybercrime strategy would nevertheless need to ensure that….evidence in relation to any crime, or that all law enforcement officers, prosecutors and judges are provided at least with basic skills in this respect….[[7]](#footnote-7)

Similar logic should have been applied to the sections dealing with forgery and uttering, appropriation, and extortion. These submission have not been accepted, and those provisions remain the same.

# State Security and its role in cybercrime.

1. National Critical Information Infrastructure

The section defining the NCII has been improved in the tabled Bill.

However, the tabling of the Critical Infrastructure Bill[[8]](#footnote-8) has created additional complications in the distinction between Critical Information Infrastructure, and Critical Infrastructure. In a memorandum on the interaction between the Bills, the Department of Justice advises

The practical effect of the integration of computer technology in critical infrastructures is that the Cyber Bill and the Infrastructure Protection Bill will, more usually than not, simultaneously apply to an identified infrastructure. In such an instance the respective components of the infrastructure must be evaluated to determine whether they are physical infrastructure or information infrastructure to determine the application of the respective Bills.

The Department places its confidence in the idea that Critical Infrastructure is susceptible to being guarded by the police, and Critical Information Infrastructure by software.

Protection measures that may be implemented to protect the physical structure in so far as it relates to infrastructure protection and information infrastructure protection may differ. Protection measures that relate to infrastructure protection are aimed at securing the physical structure itself. Protection measures in respect of information infrastructure are aimed at securing data, programmes, networks and devices at a physical infrastructure.

The political difference is that Critical Infrastructure is secured by the police, and Critical Information Infrastructure by State Security. There is a distinct lack of clarity in the division of jurisdiction in the Bills.

# Technical issues

1 Software tools

Sec 4 of the draft Bill makes people criminals because they have the tools of the trade for IT security, and might have the intention of misusing them, and then in addition makes them liable if they manufacture, assemble, obtain, sell, purchase, make available or advertises any such software or hardware tool.

1. http://www.justice.gov.za/legislation/acts/2000-004.pdf [↑](#footnote-ref-1)
2. https://www.gov.za/sites/www.gov.za/files/Act%2017%20of%201956\_1.pdf [↑](#footnote-ref-2)
3. https://pmg.org.za/call-for-comment/484/ [↑](#footnote-ref-3)
4. http://www.justice.gov.za/legislation/acts/2002-070.pdf [↑](#footnote-ref-4)
5. https://www.coe.int/en/web/cybercrime/the-budapest-convention [↑](#footnote-ref-5)
6. <http://www.governmentpublications.lib.uct.ac.za/news/national-cybersecurity-policy-framework-south-africa> [↑](#footnote-ref-6)
7. <https://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf> [↑](#footnote-ref-7)
8. http://pmg-assets.s3-website-eu-west-1.amazonaws.com/B\_22\_-\_2017\_critical\_infrastructure\_protection.pdf [↑](#footnote-ref-8)