PO Box 1560, Parklands, 2121 • Tel +2711 788 1278 • Fax +2711 788 1289
Email info@mma.org.za • www.mediamonitoringafrica.org
Promoting human rights and democracy through the media since 1993

8 March 2019

TO: SELECT COMMITTEE ON SECURITY AND JUSTICE
NATIONAL COUNCIL OF PROVINCES
C/O Mr G. Dixon
E-mail: gdixon@parliament.gov.za

CYBERCRIMES BILL [B6B-2017]:
WRITTEN SUBMISSION BY MEDIA MONITORING AFRICA TO THE SELECT COMMITTEE ON SECURITY AND JUSTICE OF THE NATIONAL COUNCIL OF PROVINCES

For more information, please contact:

WILLIAM BIRD, Director of Media Monitoring Africa
E-mail: williamb@mma.org.za
Tel: +2711 788 1278

THANDI SMITH, Head of Policy Programme
Email: thandis@mma.org.za
Tel: +2711 788 1278

Media Monitoring Africa was assisted in the drafting of these written submissions by ALT Advisory:
https://altadvisory.africa

CONTENTS

INTRODUCTION

1. Media Monitoring Africa (MMA) provides this submission on the Cybercrimes Bill B6B-2017, in response to the call for submissions by the Select Committee on Security and Justice (Select Committee) of the National Council of Provinces.

2. MMA has previously engaged on a number of occasions in the public participation process relating to the Cybercrimes Bill. This includes the following:

    2.1. On 30 November 2015, MMA provided written submissions to the Department of Justice and Constitutional Development on the 2015 version of the Bill.

    2.2. On 8 August 2017, MMA provided written submissions to the Portfolio Committee on Justice and Correctional Services (Portfolio Committee) of the National Assembly, in which MMA highlighted a number of concerns with various sections of the 2017 version of the Bill.

    2.3. Thereafter, on 21 September 2017, MMA presented oral submissions to the Portfolio Committee, based on the written submissions that had been provided.

    2.4. Following the presentation to the Select Committee, MMA was requested to provide supplementary written submissions with suggested textual wording in respect of particular submissions. This was submitted by MMA on 5 October 2017.

    2.5. MMA has also made written and oral submissions to the Independent Communications Authority of South Africa (ICASA) on the discussion document on the roles and responsibilities of ICASA in respect of cybersecurity.

3. MMA therefore welcomes this opportunity to make submissions to the Select Committee. As a point of departure, MMA commends the important strides that have been made in respect of the Cybercrimes Bill, in particular the removal of the sections on cybersecurity and critical information infrastructure. MMA notes that these important amendments bring the Cybercrimes Bill closer in line with our constitutional dispensation.

4. However, as set out in more detail below, there remain concerns with the Cybercrimes Bill in its current form. This submission is structured as follows:

4.1. **First**, an overview of MMA.

4.2. **Second**, the Socio-Economic Impact Assessment System (SEIAS).

4.3. **Third**, proposed amendments to the sections regarding malicious communications.

4.4. **Fourth**, the constitutional imperative that the best interests of the child must be of paramount importance.

4.5. **Fifth**, the need for a public interest override.

4.6. **Sixth**, the proposed establishment of the Interdepartmental Steering Committee on Internet Governance.

5. This is dealt with in turn below.

OVERVIEW OF MEDIA MONITORING AFRICA

6. MMA is a not-for-profit entity that has been monitoring the media since 1993. We aim to promote the development of a free, fair, ethical and critical media culture in South Africa and the rest of the continent. The three key areas that MMA seeks to address through a human rights-based approach are, media ethics, media quality and media freedom.

7. In the last 25 years, we have conducted over 200 different media monitoring projects – all of which relate to key human rights issues, and at the same time to issues of media quality. MMA continues to challenge media on a range of issues, always with the overt objective of promoting human rights and democracy through the media. In this time, MMA has consistently sought to deepen democracy and hold media accountable through engagement in policy and law-making processes.

8. MMA has made submissions relating to public broadcasting, online content regulation, cybercrimes, data protection and various other matters relevant to the exercise of freedom of expression and other information rights, both on- and offline. In this regard, MMA has presented on a number of occasions to the National Assembly and the National Council of Provinces. In addition, MMA has made submissions to broadcasters, the Press Council, the South African Human Rights Commission and ICASA. MMA also actively seeks to encourage ordinary citizens to engage in the process of holding media accountable through the various means available.

9. MMA is currently working with the Independent Electoral Commission of South Africa to develop strategies to address disinformation in the upcoming elections. MMA welcomes the removal of the criminalisation of false news from the malicious communications section of the Cybercrimes Bill. We note in this regard that criminalising speech has the serious potential to have a chilling effect on the right to freedom of expression. MMA is of the firm view that other appropriate measures exist that can serve to address disinformation intended to cause harm, without unjustifiably limiting the right to freedom of expression.

10. For more about MMA and our work, please visit: www.mediamonitoringafrica.org.

SOCIO-ECONOMIC IMPACT ASSESSMENT

11. As MMA has previously noted in the submissions to the National Assembly, following the establishment of the SEIAS by the Cabinet in February 2007, from 1 October 2015 any Cabinet Memoranda seeking approval for draft policies, bills, or regulations must include a socio-economic impact assessment compiled and approved by the SEIAS Unit.[1] The SEIAS, which replaces the Regulatory Impact Assessment, aims to "minimise unintended consequences from policy initiatives, regulations and legislation, including unnecessary costs from implementation and compliance as well as from unanticipated outcomes", and "to anticipate implementation risks and encourage measures to mitigate them".[2]

12. However, despite repeated submissions in this regard, MMA has still not had sight of any impact assessment for the Cybercrimes Bill. Indeed, when MMA raised this concern during the oral submissions to the Portfolio Committee, it became apparent that the members of the Portfolio Committee had also not had sight of the socio-economic impact assessment.

13. In terms of the *SEIAS Guidelines*, the system applies to "new or to be amended primary legislation, although the impact assessment need not be published for matters affecting national security."[3] MMA submits that the scope of the Cybercrimes Bill is far broader than the protection of national security and therefore an impact assessment needs to be conducted and made public.

[1] Department of Planning, Monitoring and Evaluation, *Socio-Economic Impact Assessment System (SEIAS): Guidelines* (May 2015) at page 3: http://www.dpme.gov.za/keyfocusareas/Socio%20Economic%20Impact%20Assessment%20System/SEIAS%20Documents/SEIAS%20guidelines.pdf.
[2] Id at page 4.
[3] Id at page 8.

14. In the even that such an impact assessment has been completed, this should be made public without delay, and stakeholders should be permitted the opportunity to make submissions on the impact assessment. The impact assessment is a self-imposed Cabinet obligation and a necessary tool in better understanding internet governance proposals within the state. In the event that an impact assessment has not been completed, further deliberations on the Cybercrimes Bill should be halted until this has been done and all relevant stakeholders have had the opportunity to consider and make submissions thereon.

THE NEED FOR A RIGHTS-BASED APPROACH

15. MMA is further concerned at the marginalisation of a rights-based approach in the Cybercrimes Bill. In addition to the SEIAS, it is critical in our view that the common point of departure for our legislation should be the Constitution and the rights enshrined within it. If we are to develop and build the society set out in our constitution it is not only logical but essential that we ensure that our laws and policies are framed within our constitution. We therefore submit that the importance of the triad of information rights - the right to privacy (section 14 of the Constitution), the right to freedom of expression (section 16 of the Constitution) and the right of access to information (section 32 of the Constitution) – are made clear as a point of departure and a central focus of the Cybercrimes Bill.

16. MMA is further concerned that the Cybercrimes Bill does not adequately acknowledge that information rights are equally applicable online as they are offline, a position that has been affirmed by both the United Nations Human Rights Council and the African Commission on Human and Peoples' Rights.[4] MMA submits that information rights, and their applicability in any cyber framework, need to be fully considered and outlined in the Cybercrimes Bill.

17. Accordingly, MMA submits that the Cybercrimes Bill should include a provision under the "Definitions and interpretation" in section 1 of the Cybercrimes Bill, along the following lines:

DEFINITIONS AND INTERPRETATION

…

(3) In undertaking any measure in terms of this Act, the State must at all times respect, protect, promote and fulfil the rights in the Bill of Rights, both online and offline, including the rights to freedom of expression, access to

[4] United Nations Human Rights Council Resolution 38/35 (July 2018); African Commission on Human and Peoples' Rights Resolution 362(LIX) (November 2016).

information and privacy, and nothing in this Act should be interpreted or relied up to unjustifiably impede the free flow of information.

AMENDMENTS TO THE SECTIONS REGARDING MALICIOUS COMMUNICATIONS

18. As an overarching principle, MMA remains concerned with the overlap of the provisions of the Cybercrimes Bill with various other laws, including the Protection from Harassment Act 17 of 2011, the Electronic Communications and Transactions Act 25 of 2002 (ECTA), POPIA and the Prevention and Combating of Hate Crimes and Hate Speech Bill. Further, in line with the submission above, MMA emphasises that the triad of information rights, including the right to freedom of expression, is of particular importance in respect of the provisions on malicious communications in light of the limitations that these provisions have the potential to impose on free speech.

19. In respect of the specific wording of the provisions in this chapter, MMA submits as follows:

    19.1. With regard to sections 17 and 18 of the Cybercrimes Bill, MMA proposes inserting the word "imminent" before all references to violence, to appropriately narrow the causal nexus between the exercise of speech and the resultant harm that the Cybercrimes Bill seeks to address.

    19.2. With regard to section 19 of the Cybercrimes Bill, MMA proposes that a requirement of harm should be inserted. This is to avoid any possible unintended consequences, such as a parent who shares a nude picture of a new born baby with family members falling foul of this provision. While such an example may be unlikely to lead to a prosecution, the concern is that this may be selectively used and thereby have a chilling effect on freedom of expression.

20. As such, and in respect of the Cybercrimes Bill in its entirety, MMA urges the drafters to carefully consider the impact of these provisions, and ensure that they are carefully and narrowly circumscribed in order to avoid ambiguity.

BEST INTERESTS OF THE CHILD

21. MMA remains concerned that the Cybercrimes Bill does not appropriately consider the best interests of the child, the use of technology to exploit children, and the low levels of digital literacy in the country. In this regard, it bears mention that the Cybercrimes Bill does not once mention "children" or "child", save for in the schedule of "Law Repealed or Amended". MMA's concerns are two-fold:

21.1. First, MMA is concerned with the possibility of children falling foul of the provisions under the Cybercrimes Bill, and being subject to criminal sanctions as a result of their immaturity or lack of understanding of the import of the Cybercrimes Bill. The Cybercrimes Bill should therefore contemplate an appropriate dispensation for children who may be in breach of its provisions. Coupled with this, it is important for there to be appropriate education and training for children on the impact of the Cybercrimes Bill, as well as other pieces of legislation that may impact children and their expression online, in order to ensure they are aware of the potential consequences. This should include curriculum development to ensure the safety and security of children online, including the impact and recourse for cybercrimes such as cyber-bullying and cyber-harassment.

21.2. Second, MMA is further concerned that the Cybercrimes Bill does not have appropriate regard to the exposure of children to pornography and the use of technology to groom and exploit children, in the light of the *South African Law Reform Commission Project on Sexual Offences: Pornography and Children*.[5] MMA submits that the protection of the best interests of the child in the context of cybercrimes should, at a minimum, be acknowledged in the Cybercrimes Bill.

22. Accordingly, in line with section 28(2) of the Constitution, which recognises that "[a] child's best interests are of paramount importance in every matter concerning the child", MMA proposes the insertion of a new section following section 19 under Chapter 3 of the Cybercrimes Bill, along the following lines:

BEST INTERESTS OF THE CHILD

(1) In applying the provisions of this Act to a child, as defined in section 1 of the Child Justice Act 75 of 2008, due regard shall be had to the best interests of the child, the age and maturity of the child, and the express intention of the child.

(2) The penalties set out in this Act do not apply to any child to whom the provisions of the Child Justice Act apply.

(3) (a) The State has a duty to promote awareness amongst children, educators, parents, guardians and other relevant persons of the provisions of this Act, and other related matters of cyber policy.

(b) Without derogating from the general nature of this duty, the Interdepartmental Steering Committee, in conjunction with the

[5] South African Law Reform Commission, Project 107, Issue Paper 30, *Sexual Offences: Pornography and Children* (5 August 2015): http://salawreform.justice.gov.za/ipapers/ip30_prj107_SexualOffences-PC-2015.pdf.

Cabinet members responsible for the administration of justice, communications, basic education, and higher education and training, must undertake the following:

(i) Conduct education and information campaigns; and

(ii) Ensure that all public officials who may be involved in the investigation and prosecution of offences under this Act are educated, informed and sensitised to the appropriate application of this Act to children.

23. Importantly, when considering the protections that Chapter 3 may aim to provide to children, particularly in the context of sexually exploitative communications and materials, care must be taken to ensure that the Cybercrimes Bill aligns with the Criminal Laws (Sexual Offences and Related Matters) Amendment Act 32 of 2007, and the Films and Publications Amendment Bill, both in terms of ensuring the relevant protections for children and in striking the appropriate balance with the right to freedom of expression.

PUBLIC INTEREST OVERRIDE

24. As MMA has previously submitted, there needs to be a deliberative move towards protecting intention, in respect of malicious communications or disclosure, where this takes place in the public interest. However, the Cybercrimes Bill still makes no reference to communications that are intentionally made available, broadcast or distributed in the public interest, the interests of justice or already in the public domain.

25. The chilling effect of this omission is that journalists or human rights defenders who publish content that falls within the scope of "malicious communications", but which may be in the public interest or in the interests of justice – such as for journalistic purposes – may still be criminally liable in terms of the CCB. To ensure the protection and promotion of the right to freedom of expression, the Cybercrimes Bill should include a public interest defence to the provisions relating to malicious communications, in an effort to ensure that members of the media and human rights defenders can perform their functions unhindered, without the risk of being intimidated by public officials or powerful individuals with the provisions of the Cybercrimes Bill.

26. Accordingly, in similar terms to the public interest override contained in the Films and Publications Act 65 of 1996, MMA proposes the inclusion of an additional sub-section to the current section 23 under the heading "Penalties", along the following lines:

PENALTIES

…

(3) The penalties contained in this Act do not apply when, judged in context, and except with respect to child pornography, the publication is a bona fide documentary, or is a publication of scientific, literary, artistic, or satirical merit, or is on a matter of public interest, or is already in the public domain.

27. By way of definition, section 1 of the Films and Publications Act defines the term "matters of public interest" as "discussions, debates or opinions on matters pertaining to the common well-being or general welfare of the public or serving the interests of the public and includes discussions, debates and opinions on matters pertaining to religion, belief or conscience". A similar definition may be considered for the Cybercrimes Bill, adapted as appropriate for the relevant context.

ESTABLISHMENT OF AN INTERDEPARTMENTAL STEERING COMMITTEE

28. It remains a key concern for MMA that there is a lack of any overarching internet governance policy in South Africa. The Cybercrimes Bill will form one more in a plethora of legislation dealing with overlapping and interrelated cyber matters, and a number of bodies with similarly unclear and overlapping mandates. In turn, rather than alleviate this concern, the Cybercrimes Bill exacerbates this concern by adding a further layer of complexity, without it being fully considered how the Cybercrimes Bill coheres with existing legislation.

29. For example, alongside the Cybercrimes Bill, the Prevention and Combating of Hate Crimes and Hate Speech Bill, the Films and Publications Amendment Bill, the Copyright Amendment Bill, POPIA, ECTA and the National E-Strategy in terms of ECTA, among others, all contain sections relevant to internet governance but do not expressly indicate how interdepartmental cooperation is going to occur for the purposes of overall internet governance policy within the state. In the absence of a clear internet governance policy and legislative guidance, an unduly complex structure of oversight is in the process of being created.

30. It is now commonly acknowledged that there are regulatory difficulties associated with technology innovation,[6] and that information rights continue to be defined and developed in the digital age. The OECD suggests that "regulatory reform is directed to making sure that regulations are fully responsive to changes in the economic, social and technical conditions surrounding them".[7] MMA's central concern, in the absence of

[6] See, for example, Organisation for Economic Co-Operation and Development (OECD), *Regulatory Reform and Innovation*: https://www.oecd.org/sti/inno/2102514.pdf.
[7] Id at page 7.

guidance from the SEIAS Unit and a clear and publicly accessible overarching internet governance policy, is that people in South Africa, civil society organisations and members of the media, among others, need to navigate an overly complex regulatory landscape in order to make submissions, conduct their business and exercise their information rights. Additionally, this poses significant challenges to government's coordinated and effective implementation of the existing regulatory provisions, and may result in overlapping mandates or aspects not being assigned or accounted for by appropriate functionaries.

31. Further, with rapid technological developments, including the development of technologies used to perpetrate cybercrimes, the complex governance structures created by the various pieces of legislation dealing with internet governance may not be amenable to swift and effective responses by the state to cybercrimes and technological developments which, in turn, may lead to a failure by the state to meet its constitutional obligation to respect, protect, promote and fulfil the rights in the Bill of Rights.[8]

32. A further constitutional consideration relates to cooperative governance and intergovernmental relations. In terms of section 41(1)(c) of the Constitution "[a]ll spheres of government and all organs of state within each sphere must provide effective, transparent, accountable, and coherent government for the Republic as a whole" and the must "co-operate with one another in mutual trust and good faith by coordinating their actions and legislation with one another".[9]

33. Accordingly, MMA proposes the establishment of the Interdepartmental Steering Committee on Internet Governance, to serve as a necessary – and arguably constitutionally required – central node within the state, as a response to bring harmony to South Africa's internet governance framework and to ensure swift and effective state responses to cybercrimes.

34. Notably, MMA proposes that the Interdepartmental Steering Committee comprise various stakeholders in addition to state functionaries, including independent experts and representatives of civil society, to ensure that there is coherence, good governance and the requisite technical expertise.

35. Accordingly, MMA proposes the inclusion of a new section along the following lines:

[8] Section 7(2) of the Constitution.
[9] Section 41(1)(h)(iv) of the Constitution.

INTERDEPARTMENTAL STEERING COMMITTEE (ISC) ON INTERNET GOVERNANCE

(1) The ISC on Internet Governance is hereby established.

(2) The ISC on Internet Governance consists of--

(a) a chairperson who is the Director-General: Department of Justice and Constitutional Development;

(b) members who are the Heads of the representative Departments and one of their nominees who must be officials--

(i) at the rank of at least a chief director or equivalent, of a representative Department, who are specifically nominated by a Head of that representative Department to serve on the ISC on Internet Governance; and

(ii) to whom a security clearance certificate has been issued by the State Security Agency in terms of section 2A of the National Strategic Intelligence Act, 1994 (Act No. 39 of 1994);

(c) members set out in sub-section (9).

(3) The Cabinet member responsible for the administration of justice must appoint a member to act as chairperson whenever the chairperson is absent from the Republic or from duty, or for any reason is temporarily unable to carry out the responsibilities as chairperson.

(4) The work incidental to the performance of the functions of the ISC on Internet Governance must be performed by a secretariat, consisting of designated administrative personnel of the Department of Justice and Correctional Services.

(5) The objects and functions are to coordinate, rationalise and implement government policy relating to internet governance, cybercrimes and cybersecurity, to undertake educational and awareness campaigns, and to assist and advise on the formulation of future policy.

(6) The Cabinet member responsible for the administration of justice must oversee and exercise control over the performance of the functions of the ISC on Internet Governance.

(7) The Cabinet member responsible for the administration of justice must, at the end of each financial year, submit a report to Parliament regarding progress that has been made towards achieving the objects and functions of the ISC on Internet Governance.

(8) For the purposes of this section--

(a) "Head of a Department" means the incumbent of a post mentioned in Column 2 of Schedule 1, 2 or 3 to the Public Service Act, 1994, and includes any employee acting in such post; and

(b) ''representative Department'' means--

(i) the Department of Defence;

(ii) the Department of Home Affairs;

(iii) the Department of International Relations and Cooperation;

(iv) the Department of Justice and Constitutional Development;

(v) the Department of Science and Technology;

(vi) the Department of Telecommunications and Postal Services;

(vii) the Financial Intelligence Centre, established by section 2 of the Financial Intelligence Centre Act, 2001 (Act No. 38 of 2001);

(viii) the National Prosecuting Authority;

(ix) the National Treasury;

(x) the South African Police Service;

(xi) the South African Reserve Bank;

(xii) the South African Revenue Service;

(xiii) the State Security Agency;

(xiv) the Information Regulator;

(xv) any other Department or public entity which is requested, in writing, by the Chairperson of the ISC on Internet Governance to assist.

(9) The ISC on Internet Governance should also comprise the following members:

(a) Two representatives from opposition parties represented in the National Assembly;

(b) Two teachers of law, or members of the attorneys' or advocates' profession, with knowledge of internet governance laws who are approved by the Chairperson of the ISC on Internet Governance following a public call for nominations;

(c) Two technical experts in internet governance who are approved by the Chairperson of the ISC on Internet Governance following a public call for nominations;

(d) Two members of civil society organisations working on internet governance who are approved by the Chairperson of the ISC on Internet Governance following a public call for nominations.

(10) The ISC on Internet Governance shall, at all times, conduct its affairs in an open, transparent and accountable manner, and be responsive to the needs of the public and to technological developments.

36. In addition to these amendments to the Cybercrimes Bill, the establishment of the Interdepartmental Steering Committee on Internet Governance would also necessitate the amendment and/or rationalisation of an array of other legislation, and regulations

and policies published thereunder, that deal with matters related to internet governance. Such amendments are necessary to ensure that the desired coordination is achieved. This may be achieved through a schedule of amendments contained as a schedule to the CCB. The necessary laws may include:

36.1. ECTA;
36.2. POPIA;
36.3. Films and Publications Act;
36.4. Copyright Act 98 of 1978;
36.5. Electronic Communications Act 36 of 2005;
36.6. Intelligence Services Act 65 of 2002;
36.7. Intelligence Oversight Act 40 of 1994;
36.8. National Strategic Intelligence Act 39 of 1994;
36.9. Financial Intelligence Centre Act 38 of 2001;
36.10. Prevention and Combating of Hate Crimes and Hate Speech Bill [2016].

CONCLUDING REMARKS

37. MMA appreciates the opportunity to provide this submission to the Select Committee, and would welcome the opportunity to make further oral submissions to the Select Committee as well. Notwithstanding the important strides that have been made on the Cybercrimes Bill, there is still work that needs to be done to ensure that the Cybercrimes Bill is effective and appropriate within our constitutional and legislative framework. Accordingly, MMA remains willing and available to assist Parliament and the Department of Justice and Constitutional Development going forward.

MEDIA MONITORING AFRICA
Johannesburg, 8 March 2019

ENDS.