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

Attention: SJ Robbertse
The Department of Justice and Constitutional Development,
Private Bag X81,
PRETORIA,
0001
Email: cybercrimesbill@justice.gov.za

30 November 2015

WRITTEN SUBMISSIONS BY THE MEDIA MONITORING AFRICA (MMA) ON THE CYBERCRIMES AND CYBERSECURITY BILL (DRAFT FOR PUBLIC COMMENT)

1. ABOUT MEDIA MONITORING AFRICA

1.1. MMA's vision is a just and fair society empowered by a free, responsible and quality media. Through a human rights-based approach, MMA aims to promote the development of:

- Media that is transparent, diverse, ethical and accountable to its audiences;
- Critical and constructive communications by the powerful; and;
- Informed, engaged and connected citizenry

1.2. MMA aims to contribute to this vision by being the premier media watchdog in Africa to promote a free, fair, ethical and critical media culture. The three key areas MMA seeks to address through a human rights-based approach are media freedom, media ethics and media quality. Established in 1993 to monitor South Africa's first democratic elections, MMA has over 20 years experience in media monitoring and direct engagement with media, civil society organisations and citizens. MMA is the only independent organisation that analyses and engages with media according to this framework. In all of our projects, we seek to demonstrate leadership, creativity and progressive approaches to meet the changing needs of the media environment.

2. INTRODUCTION

2.1. The Department of Justice and Constitutional Development (DOJ & CD) published the Cybercrimes and Cybersecurity Bill (the Bill) and invited interested persons to make written representations by the 30th of November 2015. MMA thanks DOG & CD for the opportunity to make this written submission and hereby request an opportunity to make oral representations at such hearings.

2.2. "The Internet is one of the fastest growing areas of technical infrastructure development. Today, Information and Communication Technologies (ICTs) are omnipresent and the trend towards digitization is growing. The demand for Internet and computer connectivity has led to the integration of computer technology into products that have usually functioned without it, such as cars and buildings"[1].

2.3. The international community has recognized the potential benefits of ICTs and encouraged governments to elaborate comprehensive, forward-looking, sustainable national ICT strategies as an integral part of their development plans and poverty reduction strategies. Many developing countries have already put in place one or several national ICT plans and others are in the process of doing so.

2.4. It is against this backdrop that Media Monitoring Africa (MMA) welcomes the call for submissions by the DOJ &CD. MMA believes that in the same way a fire can only exist with three key elements (air, heat and water) in order for a democracy to thrive, it is essential that there is freedom of expression. For freedom of expression to be realised, there are three key elements which cannot be ignored. The three key elements include that of; Access to information; Transparency (institutions, processes and people) and Accountability mechanisms.

2.5. The above elements offer context relating to media and ICT freedom which are key elements of a democracy. We cannot therefore look at Cybercrimes and Cybersecurity and ignore Media Freedom. The Bill has to be in line with our Constitution that clearly protects Freedom of Expression and Media Freedom.

2.6. MMA also believes that South Africa and the African continent can learn from the mistakes made from countries that are further developed technologically and instead of making the same mistakes, we are able to 'leapfrog' ahead and implement a Cybercrimes and Cybersecurity law that is far greater and far more advanced than policies implemented before this.

3. OVERALL IMPRESSIONS OF THE BILL

3.1. MMA is aware that at present, South Africa has no legislation that addresses Cybercrimes and Cybersecurity, whether it is to describe what constitutes a Cybercrime, how to enforce

[1] Read "Understanding Cybercrime: Phenomena, Challenges and legal responses available online: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

the law governing Cybercrime, or to determine appropriate correctional sentencing for those convicted of offences in this realm.

3.2. The Bill is timeous in that it proposes legislation that will bring South Africa in line with international laws governing internet-based crimes. However, the Bill is excessively far-reaching, not practical and in many instances it grants a concerning level of discretion to the South African Police Service and the State's security cluster.

3.3. This is not to say that the entire Bill is not necessary or is bad; there are sections in the Bill of which MMA is fully supportive. Section 3 for example specifically addresses the unlawful acquisition of personal and financial information with the intention of committing an offence, and it is linked to the Protection of Personal Information Act of 2013. Similarly, Section 9 addresses unlawful acts in respect of malware, Section 10 addresses the unlawful acquisition or access to passwords and access codes, and Section 20 addresses copyright.

3.4. One of the key concerns MMA has around the Bill is the ambiguities in several of the definitions. A particularly stark example is the definition of what exactly constitutes 'critical data'. The ambiguities are bread and butter for conspiracy theorists who would suggest dark and underhanded intentions in putting the bill forward. MMA fully supports and calls legislation that is in line with best international democratic practice; MMA encourages the department to caution against creating an impression that computers and online technology have only negative consequences. Not only would such a view discourage users but also investors.

4. LAW IS ISOLATED

4.1. MMA is fully aware that the technological developments associated with cybercrime mean that, while current laws can be applied it is also important that legislation come to grips with new concepts and objects that are not covered by the current laws. We are also very aware that legal measures are crucial to the prevention and combating of cybercrime.

4.2. In its current form the Bill appears to be in isolation not only of other pieces of legislation but other critical development and issues in the sector. A clear and critical example is Section 3.2.1 in the explanatory note and section 20 of the Bill which both deal with Copyright. Neither of the sections in any way recognises nor refers to existing laws that deals with copyright. Further, no mention is made regarding the pending changes to the Copyright Act. This omission could result in a contradiction, a lacunae or simply confusion about the law. In so doing instead of bringing about much needed action and clarity it may result in delays and unfair treatment.

4.3. Equally concerning for MMA is the lack of acknowledgement and synergies around the work of other departments who are also seeking to bring clarity and purposes to the ICT framework and sector. Even though it is important to have legislation around cybercrimes, for the legislation to be comprehensive, inclusive, transparent, and in the public interest, it

is important that it does not ignore other efforts such as those made by the Department of Telecommunication and Postal Services, which is in a process of an ICT Policy Review[2].

5. DEFINITIONS

5.1. As indicated, there are serious concerns around some of the definitions in the Bill. Some of the definitions are not only broad, but also not practical and there is lack of clarity of what exactly the Bill is trying to criminalise or what is exempted. MMA supports completely section 3 of the Mozilla submission. We would like to reiterate the following:

5.2. Electronic Communications Service Provider

An electronic communications service provider (ECSP) is defined in section 1 as follows:

"Electronic communications service provider" means any—

(a) person who provides an electronic communications service under and in accordance with an electronic communications service licence issued to such person under Chapter 3 of the Electronic Communications Act, 2005 (Act No. 36 of 2005), or who is deemed to be licensed or exempted from being licensed as such in terms of the Electronic Communications Act, 2005;

(b) 'financial institution' as defined in section 1 of the Financial Services Board Act, 1990 (Act No. 97 of 1990); or

(c) person or entity who or which transmits, receives, processes or stores data—

(i) on behalf of the person contemplated in paragraph (a) or (b) or the clients of such a person; or

(ii) of any other person;

Under clause (a), an ECSP includes anyone who provides an electronic communications service. Such a service is defined in the Electronic Communications Act, 2005 as: any service provided to the public, sections of the public, the State, or the subscribers to such service, which consists wholly or mainly of the conveyance by any means of electronic communications over an electronic communications network, but excludes broadcasting services;

These services can be licensed or exempt from licensing, but the Cybercrimes Bill's definition of ECSP covers providers of both. So the definition of ECSP includes anyone who has installed a public wireless access point, anyone involved in a community mesh network, libraries, formal and informal Internet cafes, anyone running peer-to-peer data sharing software and almost anyone running a network server - which is increasingly something Internet users wish to do from home.

Furthermore, under clause (c) (ii), ECSP includes any person who transmits, receives, processes or stores the data of "any other person." Any interaction over the Internet includes receiving data belonging to someone else - e.g. when you visit a website, you download the website's

[2] Read MMA's written submission on the ICT Policy Review here: http://www.mediamonitoringafrica.org/index.php/resources/entry/mmas_submission_in_response_to_the_ict_green_paper_2014/

copyrighted data in order to view it. An email you receive is data which was authored by and belongs to someone else. So, according to this definition, everyone who accesses information or services via the Internet becomes an ECSP.

This seems to be a case of clear, albeit unintentional, overbroad definition. The requirements placed on an ECSP in section 64 are aimed at ECSPs providing a commercial service and with whom the customer has an ongoing and probably financial relationship. At minimum, the definition should be tightened to include only such ECSPs.

5.3. National Critical Information Infrastructure

National Critical Information Infrastructure is defined in section 1 as follows: "National Critical Information Infrastructure" means any data, computer data storage medium, computer device, database, computer network, electronic communications network, electronic communications infrastructure or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto—

(a) which is specifically declared a National Critical Information Infrastructure in terms of section 58(2) of this Act; or

(b) which, for purposes of Chapters 2 and 4 of this Act, are in possession of or under the control of—

(i) any department of State or administration in the national, provincial orlocal sphere of government; and

(ii) any other functionary or institution exercising a public power or performing a public function in terms of any legislation, irrespective whether or not it is declared a National Critical Information Infrastructure as contemplated in paragraph (a);

Clause (a) allows the Cabinet member responsible for State Security to designate anything as NCII as long as it meets one of six conditions outlined in section 58. These are generally reasonable, although condition (d) ("causes any major economic loss") could be very broadly interpreted.

The problematic breadth is mostly in clause (b), which states that almost anything computer-related, including all the buildings containing any sort of network, belonging to provincial or local government or any NGO or other body which has been given any sort of responsibility whatsoever in law (it's almost certainly impossible to even list them all) is also NCII.

This is not a useful definition of the word "Critical." If everything is critical, then in practice, nothing is. It is also not reasonable to have a definition where the NCII status of something cannot be determined without encyclopaedic knowledge of the South African statute book.

Furthermore, most offences in the bill are worded such that the maximum sentence is doubled if NCII is involved. The over-broad definition of NCII means that penalties which are intended to be

exceptional will end up being commonplace - contributing to a culture of fear surrounding the use of computers generally.

5.4. Malware

Malware is defined in section 9.4 as:

any data, electronic, mechanical or other instrument, device, equipment, or apparatus that is designed specifically to—

(a) create a vulnerability in respect of;

(b) modify or impair;

(c) compromise the confidentiality, integrity or availability of; or

(d) interfere with the ordinary functioning or usage of, data, a computer device, a computer network, a database, a critical database, an electronic communications network, or a National Critical Information Infrastructure.

Clause 9.4 (b) says that malware is anything that is designed specifically to… modify… data. Therefore, by this definition, every computer or piece of software ever written is malware.

Even if the word "modify" was removed, there are a number of legitimate computer functions which would still fall under this definition. Ad blockers, for example, "interfere with the ordinary functioning of" web browsers in order to stop them downloading ads. Secure delete tools clearly "impair" or "compromise the availability of" data - that's the point of them. A security monitor on a network may "interfere with the ordinary functioning of" another network device or program by shutting it down if it suspects that it has been exploited or misused.

We can see the problematic nature of the broadness here when we notice that given the definition of National Critical Information Infrastructure to include buildings, and the definition of malware to include "mechanical or other instrument", a pneumatic drill fits this definition of malware.

Even if we take less extreme examples than this, this is clearly unintended over-criminalization. Defining malware is admittedly not simple, which is why computer professionals often talk about programs whose classification is difficult as "greyware." But this definition is too broad and needs to be significantly narrowed.

6. CYBERCRIMES AND FREEDOM OF SPEECH

6.1. In addition to the definitions that are not only broad but create a level of liability, not only to users but service providers, MMA is concerned that the is very little reference or even acknowledgement to freedom of speech. This is not to argue that freedom of speech triumphs all other rights but to emphasise the point stated earlier that the Bill cannot be in isolation. It needs to be in line with all the rights that are protected by the Bill of Rights.

6.2. MMA also believes that to ignore freedom of speech is to ignore the basic principle of most laws, that the same rights that people have offline must also be protected online.

6.3. What the Bill is also ambiguous on is the dissemination of hate speech. Section 17 of the Bill prohibits dissemination of data messages that advocates, promotes or incites hate, discrimination or violence. Whilst this is necessary it is too broad. What does the Bill mean exactly by "Advocate"? MMA believes that this section needs to be in line with the constitution and there is also a need to acknowledge other laws that deal with hate speech, including but not limited to the Equality Act.

7. TERRORISM

7.1. MMA is also concerned about Section 15: 5(b) of the bill that states the following:

> *"threaten the unity and territorial integrity of the Republic;*
> *(ii) intimidate, or to induce or cause feelings of insecurity among members of the public, or a segment of the public, with regard to its security, including its economic security, or to induce, cause or spread feelings of terror, fear or panic in a civilian population; or*
> *(iii) unduly compel, intimidate, force, coerce, induce or cause a person, a government, the general public or a segment of the public, or a domestic or an international organisation or body or intergovernmental organisation or body, to do or to abstain or refrain from doing any act, or to adopt or abandon a particular standpoint, or to act in accordance with certain principles"*,

This section suggests that anyone who writes a piece critical of the SA economy or other sectors could easily be punished as a terrorist.

7.2. While it is clear that Terrorism needs to be combated, what is not clear from this section is whether streaming a film like "Don't Mess with the Zohan" which pokes at Terrorists or "Four Lions" which is a black comedy fall foul of the section?

8. INTENTION VS. PUBLIC INTEREST

8.1. The entire Bill loosely uses the words 'unlawful' and 'intentionally' and for the entire bill, these words are the only words standing between a lawful person, organizations, businesses and criminals. The use of these words without enough clarity creates an impression that everyone that uses any device that involves data that is in any digital form can potentially be criminalized.

8.2. MMA strongly believes that even though there is a need to have a clear definition of intention there is also a need to be a deliberate move towards protecting intention that is in the public interest. We propose that the bill includes a public interest clause that will protect anyone that is in possession of data and/or critical data that is in the public interest. This we strongly believe is crucial not only for the advancement of our democracy but for the protection of those that can assist in combating crimes such as corruption.

8.3. In addition MMA submits that it is imperative that allowance is also made where there is an absence of intention, for example spreading of malware through a user's lack of knowledge or awareness of even gullibility.

9. CHILDREN AND ICTs (DIGITAL LITERACY)

9.1. The Bill fails to take into consideration the issue before the Law Reform Commission project focused on Sexual Offences Pornography and children. It is critical that the Cyber Crimes Bill speaks to these issues. While it may be necessary for these and related crimes to be dealt with separately, for 35% of our population and criminal issues' relating to them to be ignored is simply not acceptable.

9.2. MMA believes that computer ethics education as well as critical digital literacy skills should be integrated into school curricula to ensure children are aware and/or have the skills to both address and know how to be safe online.

9.3. The challenge of cyber bullying also needs to be considered and SAPS bodies must be equipped to deal with and support children who have been victims of cyber bullying.

10. CONCLUSION

10.1. The possibility exists that new forms of cybercrime will emerge with evolving technology. New cyber laws should therefore be introduced to respond to these rapid changes, especially as they will impact different sectors and groups differently. In this regard it is critical that children and marginalised groups including women's needs and issues are highlighted to ensure laws work to protect them and promote their rights. We also draw attention to the fact that the needs of other women and girls are also ignored in the Bill. Issues of online gender based violence need to be addressed.

10.2. There should also be continuous research and training of IT security personnel, finance services sector personnel, police officers, prosecutors and the judiciary to keep them abreast of advancing computer technology. At the end of the day, a balanced approach that considers the protection of fundamental human rights and the need for the effective prosecution of cybercrimes is the way forward.

MMA looks forward to participating in the oral hearings on the Bill.

FOR MORE INFORMATION PLEASE CONTACT

William Bird (Director)
williamb@ma.org.za

OR
Carol Mohlala (Project Coordinator)
carolm@mma.org.za