MOBILE TELEPHONE NETWORK PROPRIETARY LIMITED
(Registration number:1993/ 001436/07)
216 14th Avenue, Fairland, 2195
Private Bag 9955, Cresta, 2118, South Africa
Tel +2711 912 3000 Fax +2711 912 4670

Ref: 201708/05/09

11 August 2017

PORTFOLIO COMMITTEE ON JUSTICE AND CORRECTIONAL SERVICES
Parliament Street
P O Box 15
Cape Town
8000

For Attention: Mr V Ramaano
Per Email: vramaano@parliament.gov.za

Dear Mr. Ramaano,

Re: MTN's written Submission on the proposed Cybercrimes and Cybersecurity Bill

Please find enclosed, MTN (Pty) Ltd and MTN Group Management Services (Pty) Ltd, (hereafter referred to collectively as "MTN"), submission on the proposed Cybercrimes and Cybersecurity Bill published in the **Government Gazette No. 40487** dated 09 December 2016.

MTN would like an opportunity to make an oral submission at the hearing the Committee may convene.

Should you have any further queries, please do not hesitate to contact the writer/s hereof.

Yours Faithfully,

Moses Mashisane
General Manager: Legal and Regulatory Affairs
MTN (Pty) Ltd

MTN's Submission
in respect of the proposed Cybercrimes and Cybersecurity Bill
Published in the *Government Gazette No. 40487*
of 9 December 2016

1. INTRODUCTION

MTN (PTY) LTD ("MTN") would like to thank the Portfolio Committee on Justice and Correctional Services for the opportunity and invitation to comment on the draft Cyber Crimes and Cybersecurity Bill published in the Government Gazette No 40487 on 9 December 2016 (hereinafter referred to as **"the Bill"**) and which was released for public comment in July 2017.

MTN fully appreciates the Governments' proactive approach and appreciates the opportunity to provide you, as we hereby do our submissions on the Cybercrimes and Cybersecurity Bill.

MTN further applauds the positive implications relating to simplified structures (24/7 point of contact) and fines/imprisonment for offenses relating to cyber-crime, child pornography and other cyber related offenses.

MTN's submissions consists of the following:

1. Section 2: General Submissions and Recommendations; and
2. Section 3: Specific Submissions and Recommendations.

2. GENERAL SUBMISSIONS AND RECOMMENDATIONS

2.1. Harmonisation with other Laws and Regulation

The Bill will amend several existing laws, which includes but is not limited to:

- Criminal Procedure Act of 1977, (hereinafter referred to as **"the CPA"**);
- South African Police Service Act of 1995;
- National Prosecuting Authority Act of 1998;
- Electronic Communications and Transactions Act of 2002, (hereinafter referred to as **"the ECT Act"**);
- Regulation of Interception of Communications and Provision of Communication Related Information Act of 2002, (hereinafter referred to as **"RICA"**;
- Criminal Law (Sexual Offences and Related Matters) Amendment Act of 2007;
- Criminal Procedure Act of 1978.

The Bill however, does not harmonise sufficiently on matters of electronic evidence production and preservation with the ECT Act.

The Review of the Law of Evidence project already being dealt with by the South African Law Reform Commission has not been referenced in the memorandum informing the Bill. It seems that there has not been sufficient or any attention paid to other projects, which cover similar ground.

The Bill does not consider the implications of access to information and data protection laws particularly the extent to which the Bill voids obligations of confidentiality and privacy, specifically relating to law enforcement and national security.

While the latest draft of the Bill makes it easier for law enforcement to get access to the real-time computer evidence required and allow for the expedited preservation of e-evidence, it should consider, as mentioned above, an individual's constitutional right to privacy, the right to dignity as well as the freedom of expression.

Furthermore, the Bill should consider the implications of the POPI Act, specifically concerning lawful processing and the offenses stipulated within that Act. We suggest that where other legislation allows for offenses, those will prevail.

2.2. Standard Operating Procedures

MTN proposes that the Standard Operating Procedures (SOP's) (Section 24) take into consideration:

2.2.1 That no action taken should impair the function of a computer or storage media;

2.2.2 That no action taken should produce the effect of disrupting the service of an Electronic Communications Service Provider (ECSP) to its customers not implicated in the offence or reducing service quality to such persons;

2.2.3 That no action taken should risk the disclosure of personal information or confidential information of any ECSP customer not implicated in the offence;

2.2.4 That no action taken should produce a limitation on the rights of customers to object to the preservation or disclosure of data provided for in other existing laws;

2.2.5 That no action taken should unduly impose financial costs and business disruption on the ECSP;

2.2.6 The manner in which evidence should be provided i.e. encrypted hard drives for electronic information, etc.

2.3. Problematic Definition of Offenses

Section 6 of the Bill, for instance, provides that unlawful interference with computer data storage medium or computer system is an offence.

MTN submit that interference is for instance identified in the Bill as:

(a) permanently or temporarily altering any resource of;
(b) or interrupt or impair (i) the functioning of; or
(c) the availability of a computer data storage medium or computer system.

Given the lack of clarity on what constitutes unlawful interference, this provision can give rise to inadvertent offences for interferences in the ordinary course of system maintenance, upgrades, testing, etc.

2.4. Clarity Required on Electronic Evidence Integrity and Availability

The Bill does not provide what constitutes acceptable standards or integrity and availability. The ECT Act does, in sections 14-17 provide for standards for originality and admissibility of electronic evidence.

MTN proposes that the Bill adopt the same standards as enunciated in Sections 14-17 of the ECT Act.

2.5. Clarity Required on Certain Definitions Provided for Within the Bill

Definitions provided for within the Bill (Chapter 1) are not aligned to global leading practice, such as the European Union Convention on Cyber Crime, European Treaty Series No. 185, **(commonly referred to as the Budapest Convention on Cyber Crime)** and could cause confusion when reflected in search warrants:

2.5.1 An *article* in the context of cybercrime offences means - data, computer program, computer data storage medium or computer system. The term is

used in a catch-all manner which leads to confusion in the application of such term in the Bill;

2.5.2 The definition of a computer includes the equipment and devices that are related to, connected with, or used with such a device. The broad inclusion of any equipment (not exclusively electronic or programmable etc.) but merely related to a computer is vague and confusing. This is likely to result in vague search warrants and directions. MTN accordingly submits that a proper definition of the term **"other equipment and devices"** be included in the Bill;

2.5.3 A computer storage medium includes a location from which data or a computer program is capable of being reproduced. This is vague, confusing, and likely to result in vague search warrants and directions;

2.5.4 The definition of output of data means having data displayed or in any other manner. MTN submits that a complete definition be included in respect of what constitutes "output of data" as well as what constitutes "display of data" and whether the definition includes a continuous transmission of the data;

2.5.5 The definition of traffic data is broadly defined to include the communication's format, duration or type of the underlying service.

2.6. Alignment to Leading Practice Frameworks and Standards

Alignment to global standards such as the National Institute of Standards and Technology (NIST) Cyber Security framework should be considered especially as many organisations are using this to guide their current cyber security strategies. In particular, concerning critical infrastructure. In this regard, it is submitted that Chapter 11, Section 4 of the Bill incorporates the standards as recommended by NIST.

3. SPECIFIC SUBMISSIONS AND RECOMMENDATIONS AS IT PERTAINS TO MTN

3.1. Chapter 5 – **Article to be searched for, accessed or seized under search warrant**

MTN submits that the authority provided to in Section 27(1)(a) of the Bill to a magistrate to be able to authorise a search and seizure warrant be removed, and that the authority only vests with the "Designated Judge" as defined in RICA.

The "designated Judge" is defined in RICA as "and judge of a High Court discharged from active service under Section 3(2) of the Judges Remuneration and Conditions of Employment Act, 2001, or any retired Judge, who is designated by the Minister to perform the functions of a designated judge for the purposes of this Act".

It is submitted that the designated Judge in terms of RICA will be in a better position to assess the merits of applications that are made for search, seizure and access warrants. It is submitted that this will also give effects to the provisions of POPIA, for the protection and confidentiality of information.

MTN further submits that Section 27 (2) (g) of the Bill permits a police official to access and seize the article in question which forms the subject of the investigation.

MTN submits that the current wording suggests that the State may seize the actual electronic communications network of an electronic communications service provider such as MTN, which is unnecessary and not practical. It is therefore concerning that such extensive seizure powers have been granted to the State through the Bill. MTN therefore submits that limitations need to be specified in the warrant and such limits should only be confined to access control information (either physical or logical access information) relating to the network of the Electronic Communications Service Provider. The rationale for this is that any cyber security threat/incident posed to the network of the Electronic Communications Service Provider will be identified and addressed in the access control layer of the network and as such the provision of the associated information should be addressed in the warrant.

The Bill also fails to take cognisance of the fact that damage can result from the unlawful seizure of information and communication technologies contemplated in section 27(2). In this regard, it must be borne in mind that most of this information is hosted on hardware supporting these technologies. Cognisance must be taken of the cautionary rules adopted by the Courts in relation to Anton Piller Orders. The effects of these provisions are that it may cause the interruption of legitimate processing of information by search and seizure operations as envisaged by the Bill.

The issue with regards to the urgency of warrants need to ensure that proper checks and balances are in place and that any person or organisation which is subject to a warrant under these circumstances is protected in relation to items seized. Against this backdrop, it is critical for businesses or any person to continue their daily operations and in the event of a seizure, this may not be possible. The Bill fails to adequately take this into account.

MTN therefore submits that limitations need to be specified in the warrant and such limits should only be confined to access control information (either physical or logical access information) relating to the network of the Electronic Communications Service Provider. The rationale for this is that any cyber security threat/incident posed to the network of the Electronic Communications Service Provider will be identified and addressed in the access control layer of the network and as such the provision of the associated information should be addressed in the warrant.

3.2. Onerous Evidence Preservation and Disclosure Obligations

3.2.1 Section 19 provides for a form of take down of data messages. According to this section, any person who lays a charge with the Police Service may apply to court for an order pending the finalisation of the proceedings to prohibit a person from making available, broadcasting or distributing the data message associated with the charge or order an ECSP or person in control of a computer system to remove or disable access to the data message.

This does not take into account data messages that are transmitted via social media sites, and due to the fact that social media sites are not managed or under the direct control of an ECSP such as MTN, it will be impossible for an ECSP to prevent the further dissemination of the data message. This is predicated by the fact that the ECSP only facilitates the data transmission via its mobile or fixed network, but is not responsible for the actual data message being transmitted.

3.2.2 Section 20 places obligations on an ECSP or person in control of computer system to furnish particulars to court (affidavit) including personal particulars of the originator of data messages and "any other information available to an ECSP which may be of assistance" to identify the originator.

As per the point above, information should be provided taking into account an individual's constitutional right to privacy, the right to dignity as well as the freedom of expression.

3.2.3 Section 32 imposes obligations on an ECSP (and other persons who are in control of data, a computer program, a computer data storage medium or a computer system), to provide technical assistance and other assistance to a police official who is authorised in terms of a warrant to conduct an investigation in order to search for, access and seize an article.

Section 33 criminalises the obstruction or hindering of a police official or investigator to conduct an investigation.

It is submitted that this could cause severe financial harm to an ECSP such as MTN, should the article seized be critical to the day to day operations of an ECSP such as MTN.

In this regard, MTN submits that provisions be made for in Section 32 for the police official to be provided with a digital copy of the information required so as to not disrupt the daily operations of an ECSP

3.3. Chapter 9 – Obligations of electronic communications service providers and financial institutions: Section 52

As per Chapter 9 of the Bill, the Cabinet member responsible for policing must make regulations prescribing the category or class of offences which must be reported to the Police in terms of section 52(2)(a); and form and manner to report offences as per section 52(2)(b).

MTN submits that it would be prudent that such regulations as contemplated in section 52 of the Bill should also uphold the confidentiality rights of the electronic communications service providers when reporting the use of its electronic communications network to the National Cybercrime Centre.

As such, section 52(2)) should therefore be amended as follows:

"The Cabinet member responsible for policing, in consultation with the Cabinet member responsible for the administration of justice must make regulations regulating the manner in which an electronic communications service provider must report the use of its computer network or electronic communications network to commit an offence, to the National Cybercrime Centre ***on a confidential basis."***

3.4. Critical Infrastructure (Chapter 11)

MTN submits that it strongly supports the consultative approach for declaring of a National Critical Information Infrastructure as contained in the Bill.

It is submitted that Chapter (11) pertaining to Critical Infrastructure is concerning in terms of:

3.4.1 In terms of the ECT Act electronic communications Information infrastructure is defined as ***"and electronic communications products or systems used to transmit and store or transmit or store critical electronic communications"***

In terms of the Bill, "information infrastructure means "any data, computer programme, computer data storage medium, computer system or any part thereof or any building, structure, facility, system or equipment associated therewith or part or portion thereof or incidental thereto"

MTN submits that due to the fact that the ECT Act also addresses certain aspects relating to cybersecurity, that the above definition of information infrastructure in the Bill be aligned to include the definitions as contained in the ECT Act.

3.4.2 The ECT Act spoke to critical databases housing essential data. The provisions of the Bill speak in broad terms to information infrastructure. Secondly, what constitutes critical information infrastructure is a departure from the definition of critical databases in the ECT Act which pertained to information that is important to national security or the socio economic well-being of citizens. The Bill speaks vaguely to infrastructure pertaining to a potential "disruption of an essential service," or "destabilisation of the economy of the Republic".

3.4.3 Section 57(4) of the Bill prescribes the processes for the issuing of minimum standards of management of the databases in the form of directives. The directives may potentially overhaul existing management (particularly information security management) approaches in order to comply with the directives.

It is submitted that the directives referred to herein may not necessarily be in line with international best standards and methodology, or in line with the owners or controllers best standards.

MTN submits that the issuing of the directives relating to minimum standards be done in consultation with the owner or controller of the critical information infrastructure, so that the standards issued will be conversant with industry specific regulations governing quality of service and non-disclosure of consumer information

3.4.4 In terms of Section 57(7), the owner or controller may dispute the decision and lodge the dispute within 30 days of the decision is made known and set out the grounds for the dispute. Dispute resolution regulations will be issued in consultation with the cabinet member responsible for administration of justice.

MTN submits that the guidelines should cater for the length of the arbitration process should a dispute be lodged. MTN accordingly recommends that provision be made for the suspension of the directive, and for all instructions in accordance with the directive to be held in abeyance pending the resolution of the dispute in accordance with the arbitration process defined under Section 57(7)(e) of the Bill.

3.4.5 In terms of Section 57(8) of the Bill, compliance with the directives is at the cost of the owner/ controller of the infrastructure in question. The Bill further stipulates that any failure to comply is an offence with a maximum 2-year imprisonment or a fine or both.

It is submitted that there are no regulatory impact assessments of the cost of compliance that have been conducted in order to assess the financial burden that may be associated with compliance with the directives proposed in the Chapter 5 of the Bill

MTN submits that in order to give effect to the directives issues in terms of Section 57 that such an assessment be done to measure the financial impact the cost of compliance will have on ECSP's.

4. CONCLUSION

MTN emphasise that addressing of cyber-related crime and offenses through a Bill is a necessary and welcomed initiative.

MTN is however concerned in the manner in which the following issues have been addressed in the Bill:-

4.1 A regulatory impact assessment has not been conducted to inter alia assess the following:

4.1.1 The cost of compliance;

4.1.2 The level of expertise available within law enforcement and other government departments to establish the cybersecurity hubs; and

4.1.3 The privacy rights as referred to in POPI vis a vis the rights conferred upon law enforcement in accordance with this Bill.

MTN proposes that these issues are of critical importance to the success and implementation of this Bill.

END