DEPARTMENT OF JUSTICE AND CONSTITUTIONAL DEVELOPMENT: REPUBLIC OF SOUTH AFRICA

CYBERCRIMES AND CYBERSECURITY BILL, 2017

Government Gazette No. 40487 of 9 December 2016

Joint Submission made on 10 August 2017

by

Contents

Introduction

1. Cell C Limited ("Cell C") prepared a written submission on the draft Cybercrimes and Cybersecurity Bill published in the Government Gazette No 40487 on 9 December 2016 (hereinafter referred to as "the Bill") which was released for public comment.

2. Telkom SA SOC Ltd ("Telkom") and Vodacom Group Limited ("Vodacom") have provided their support to the submissions prepared by Cell C, as well as additional comments. The submissions contained herein is based on what was prepared by Cell C and supplemented by the other two (2) operators and input and comments from hereon will be referred to as input and comments from the three Mobile Network Operators ("the MNOs").

3. The MNOs wish to thank the Portfolio Committee on Justice and Correctional Services for the opportunity and invitation to provide our joint comments on the Bill.

4. The MNOs also welcome the consideration and in some instances inclusion of comments that were made on the 2015 draft of the Bill. Our joint comments included on the 2017 version of the Bill serves to highlight areas where we have firstly agreed with the content of the Bill and secondly, where we either jointly or severally raised our views on provisions that we submit need to be addressed.

5. The MNOs view this Bill as an important step in addressing the rising threat of cybercrime to our country. It is our understanding that the Bill aims to rationalise the laws of South Africa that relate to cybercrime and cybersecurity into a single Bill, thus addressing the current fragmentary approach and also further aligning our legislative framework to international standards such as the Council of Europe Convention on Cybercrime[1] (commonly referred to as the Budapest Convention on Cybercrime).

6. As a collective, the MNOs wish to commend the Department of Justice and Constitutional Development (DoJ & CD) on *inter alia* the following positive changes that will be brought about by the Bill:

6.1 Recognition of the socio-economic impact of cybercrime on South Africa as a country and the need to deal with cybercrimes in a separate Bill. As per a media statement made on 19 January 2017 by the Deputy Minister of Justice and Constitutional Development, the Hon JH Jeffery, MP (the Honourable Minister):

> *… cybersecurity plays an important role in the ongoing development of information communication technology. Enhancing cybersecurity and protecting critical information*

infrastructures are essential to each nation's security and the economic well-being of a country."

6.2 Recognition of the need for structures to more effectively facilitate international responses to cybercrime incidents such as *inter alia* the 24/7 Point of Contact, the Cybersecurity Hub and Cyber Incident Response Teams, which are also aimed at promoting cybersecurity and capacity building.

6.3 Recognition of cyber offences such as theft of an incorporeal, the distribution of certain malicious communications, cyber harassment, harmful disclosure of pornography (so-called *revenge porn*), addressing child pornography (both in the *real* and *virtual* world).

6.4 Imposition of penalties that take cognisance of the impact and seriousness of cyber-related offences.

6.5 Regulation of jurisdiction to provide for and recognise that cybercrimes are more often than not borderless crimes. Coupled with this the Bill also regulates mutual assistance to deal with cross-border investigation of cybercrimes.

6.6 Providing for the identification and declaration of critical information infrastructures and implementation of measures to protect critical information infrastructures.

7. For purposes of this document, our submissions will be categorised as follows:

7.1 Section 1: South African Legislative Framework

7.2 Section 2: Chapter by Chapter Submissions and Recommendations on the Bill

8. Cell C, Vodacom and Telkom would like an opportunity to make oral submissions on the Bill, should there be public hearings and to participate in any further consultations in this regard.

1. Section 1: South African Legislative Framework

1.1 General Remarks

1.1.1 The Department of Justice and Constitutional Development (DoJ & CD) has been tasked with the review and alignment of cybersecurity laws to ensure that these laws are aligned with the National Cybersecurity Policy Framework (NCPF) and provide for an integrated cybersecurity legal framework for South Africa.

1.1.2 As per a media statement made on 19 January 2017 by the Honourable Minister, the new proposed Cybercrime and Cybersecurity Bill will give effect to this mandate. The MNOs agree with the submission of the Honourable Minister that deterring cybercrime is a vital component of a national cybersecurity and critical information infrastructure protection strategy and that the Bill aims to advance these objectives. The Bill will thus *inter alia*, act as a deterrent to criminal elements that commit cybercrimes against our country and citizens, as well as offer protection to the State, its citizens and its resources.

1.1.3 The MNOs also take note that the Bill aims to create a centralised point for offences related to cybercrimes and to do away with the fragmented approach in our South African law pertaining to cybercrimes. We furthermore note that where a person is prosecuted for an offence in terms of the Bill, the State must still prove the elements of an offence beyond reasonable doubt as is required in terms of the adversarial criminal justice system of the South African law.

1.1.4 In addition it is our submission that, save where otherwise cautioned, we did not find anything in the Bill in contradiction with the presumption of innocence that has been emphasised by our courts: acts have to be criminalised and have to be committed with a *criminal* intent.

1.1.5 Clause 61 of the Bill repeals or amends the following laws:

- South African Police Service Act, No. 68 of 1995
- Criminal Procedure Act, No. 51 of 1977
- Criminal Law Amendment Act, No. 105 of 1997
- National Prosecuting Authority Act, No. 32 of 1998
- Correctional Services Act, No. 111 of 1998
- Financial Intelligence Centre Act, No. 38 of 2001
- Electronic Communications and Transactions Act, No. 25 of 2002

- Disaster Management Act, No. 57 of 2002
- Protection of Constitutional Democracy against Terrorist and Related Activities Act, No. 33 of 2004
- Films and Publications Act, No. 65 of 1996
- Criminal Law (Sexual Offences and Related Matters) Amendment Act, No. 32 of 2007
- Child Justice Act, No. 75 of 2008
- Regulation of Interception of Communications and Provision of Communication related Information Act, No. 70 of 2002 (RICA)

1.1.6 It is the MNO's submission that although there are laws dealing with the submission of electronic evidence in civil and criminal proceedings, these can be improved to cater for technological advances. We are furthermore aware that the South African Law Reform Commission (SALRC) is currently conducting a review of the Law of Evidence and would advise that this be taken into account insofar as it applies to electronic evidence in criminal proceedings prior to finalisation of the Bill.

1.2 Identity Theft

1.2.1 Many forms of cybercrime relate to identity theft in one way or the other. Identity theft can actually be viewed as the key offence from which many other crimes can follow. It is the MNOs submission that whether identity theft is defined as the stealing of personal information to commit fraud, misusing the identity of another person (his/her name, date of birth, address, financial information or other personal details or any combination thereof) without his/her consent, or even the theft or assumption of a pre-existing identity or any significant part thereof with or without consent, and regardless of whether the person is dead or alive – identity theft remains a global issue and more often than not is a transnational crime: information can be *harvested* in one country and used in another to commit crime.

1.2.2 Identity theft and coupled therewith subscription fraud remains the biggest fraud risk that mobile network operators in South Africa are currently facing.

1.2.3 Identity theft can be divided into three (3) distinct phases, namely:

1.2.3.1 The obtaining of identity information, for example though physical theft, through search engines, insider attacks, attacks from the outside (illegal access to computer systems, Trojans, key loggers, spyware and other malware), or phishing and other social engineering techniques.

1.2.3.2 The possession and disposal of identity information, which includes the sale of such information that now plays an important role in the e-underground economy where credit card information, bank account details, passwords or full identities are among the most offered goods.

1.2.3.3 The use of identity information in order to commit fraud or other crimes, for example by assuming another person's identity to exploit bank accounts and credit cards, create new accounts, take out loans and obtain credit, order goods and services or to disseminate malware.[2]

1.2.4 As stated above, phishing is an example of social engineering techniques used to deceive users, and exploits weaknesses in current web security. Phishing has become a key tool deployed by criminals in South Africa to fraudulently acquire sensitive information (such as passwords or other personal or financial information or data) by masquerading as a trustworthy person or business (e.g. financial institution) in a seemingly official electronic communication.

1.2.5 In the Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft by the European Commission[3], various recommendations were made on how to deal with identity theft, which included specific legislation to deal with the issue. The overall conclusions of the study were as follows regarding specific legislative measures:

1.2.5.1 Stolen data that is used maliciously (either directly by the person who *stole* it or by a third party that acquired it) has impact on individuals, businesses and/or public sector institutions.

1.2.5.2 Online identity theft accounts for the majority of cases.

1.2.5.3 The motivation for criminals to obtain identity information is due to the benefits (in particular of financial nature) for them.

1.2.5.4 Identity-related information is used mostly for financial fraud and money laundering.

1.2.5.5 Identity theft and identity-related crime affects a considerable proportion of the population, and is on the increase. It was estimated that 8.2 million individuals are affected by identity theft (2% of the EU's population) with an average loss of around €2,500 or €20bn at the EU level.

1.2.5.6 In addition to the loss of money, identity theft can have non-financial consequences for victims.

1.2.5.7 Only a few countries specifically criminalise identity related offences, but many countries criminalise it through fraud.

1.2.5.8 Identity theft, in so far as it relates to Europe, has a cross-border dimension.

1.2.5.9 The absence of a common definition hampers the development of a strategy at EU level to combat identity theft.

1.2.6 The 2015 Bill proposed amendments to the Protection of Personal Information Act, 2013, in order to address identity theft. However, these amendments were removed from the Bill on the basis that the proposed amendments may be too wide and may have unintended consequences. It is the MNO's submission that the crime of Identity Theft should be included in the Bill again.

1.2.7 The MNOs furthermore propose that when reference is made to *personal information* it is understood to mean personally identifiable information which can be used alone or in combination with other information to identify an individual and that reference to the definition in section 1 of the Protection of Personal Information Act, No. 4 of 2013 (POPIA) for purposes of a definition for the Bill would suffice. Subsection (c) Financial Information, which is referenced to in the definition of personal information in section 1 of POPIA, means any information or data which can be used to facilitate a financial transaction.

1.2.8 It is our submission that in many instances the crime of identity theft precedes that of unlawful securing of access, and thus should be inserted as Clause 2 in Chapter 2. The MNOs thus propose the inclusion of the following Clause in the Bill:

Personal and financial information or data related offences

2. (1) Any person who intentionally and unlawfully—

(*a*) acquires by any means;

(*b*) possesses; or

(*c*) provides to another person,

the personal information of another person for purposes of committing an offence under this Act or any other law is guilty of an offence.

(2) Any person who intentionally and unlawfully—

(*a*) acquires by any means;

(*b*) possesses; or

(*c*) provides to another person,

the financial information of another person for purposes of committing an offence under this Act or any other law is guilty of an offence.

(3) Any person who intentionally and unlawfully uses the personal information or financial information of another person to commit an offence under this Act or any other law is guilty of an offence.

(4) Any person who is found in possession of personal information or financial information of another person in regard to which there is a reasonable suspicion that such personal information or financial information–

(*a*) was acquired, is possessed, or is to be provided to another person for purposes of committing an offence under this Act or any other law; or

(*b*) was used or may be used to commit an offence under this Act or any other law, and who is unable to give a satisfactory exculpatory account of such possession, is guilty of an offence.

(5) Any person who contravenes the provisions of subsection (1), (2) or (4) is liable, on conviction to a fine not exceeding R5 million or to imprisonment for a period not exceeding 5 years or to both such fine and imprisonment.

(6) Any person who contravenes the provisions of subsection (3) is liable, on conviction to a fine not exceeding R10 million or to imprisonment for a period not exceeding 10 years or to both such fine and imprisonment.

(7) For purposes of this section—

(*a*) "**personal information**" means any 'personal information' as defined in section 1 of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013); and

(*b*) "**financial information**" means any information or data which can be used to facilitate a financial transaction.

2. Section 2: Chapter by Chapter Submissions and Recommendations on the Bill

2.1 Ad Chapter 1: Definitions

2.1.1 Although there is no definition of *cybercrime* in the Bill, the Memorandum on the Objects of the Cybercrimes and Cybersecurity Bill, 2017 (the Memorandum) refers to an attempted definition of cybercrimes as crimes which are committed by means of, or which were facilitated by or which involve data, a computer program, a computer data storage medium or a computer system. Cybersecurity is defined as technologies, measures and practices

designed to protect data, computer programs, computer data storage mediums or a computer systems against cybercrime, damage or interference.

2.1.2 Other than the issues raised above, wording of definitions pertaining to *computer* should otherwise be cognisant of the fact that *computer* can no longer commonly be described as a *device* but may otherwise also be a *software image* that in its entirety emulates all the functions of a computer by means of *virtualisation* and within such software image, programs, data and storage can be contained.

2.1.3 The question was, however, raised whether or not the definitions of *computer* or *computer system* accounts for the concept of Network Function Virtualisation (NFV) where it may not be possible to discern where the *computer* or *computer system* was present at the precise time of the incident.

2.1.4 For reasons of consistency the Bill should not leave the classification of devices such as smartphones or tablets as *computers* or *computer systems* or not by interpretation of the nomenclature in this Bill, to police officials or possibly misconstrued public consensus. Such classification should at least be covered in training and be incorporated in Standard Operating Procedures.

2.2 Ad Chapter 2: Cybercrimes

2.2.1 Offences against the Integrity, Confidentiality and Availability of Data, Computer Programs, Data Storage Mediums and Computer Systems

2.2.1.1 Some of the offences dealt with in the Bill were already in existence under Chapter XIII of the ECT Act, No. 25 of 2002 such as unauthorised access to, interception of, or interference with data and computer-related extortion, fraud and forgery.

2.2.1.2 Clause 2(1) deals with the unlawful securing of access and stipulates that any person who unlawfully and intentionally secures access to data, a computer program, a computer data storage medium, or a computer system, is guilty of an offence. The access must furthermore be unauthorised. Clause 2(3) further defines unauthorised access.

2.2.1.3 The MNOs submit that the offence of unlawfully securing access as per Clause 2(1) is aligned to international best practice and necessary in view of the rise of this type of offences that we have dealt with. This type of conduct typically leads to the commission

of various other types of cyber offences. But, as stated above, it is our submission that this offence should be preceded by the offence of Identity Theft in Chapter 2 of the Bill.

2.2.1.4 Unlawful Acquisition of Data

2.2.1.4.1 Clause 3 deals with the unlawful acquisition of data. It is our understanding that Clause 3 aims to protect data which is stored or transmitted over an electronic communications system and to criminalise conduct which is aimed at overcoming protection measures which are intended to firstly prevent access to data and thereafter the acquisition of such data. Clause 3 further criminalises -

- the possession of data, with the knowledge that such data was acquired unlawfully; and
- possession of data, in regard to which there is a reasonable suspicion that such data was acquired unlawfully where the possessor is unable to give a satisfactory exculpatory account of such possession.

2.2.1.4.2 The MNOs further propose that Clause 3 should be adopted in line with the international position which deals with the *interception of data to, within or from an electronic communications system*. Although the current clause does address this aspect, international co-operation and future development of the law relating to cybercrime will greatly be facilitated if offences are worded similarly to that of the international community.

2.2.1.4.3 The use of information communication technology is accompanied by several risks related to the security of information transfer. Unlike classic mail-order operations, data-transfer processes over the Internet involve numerous providers and different points where the data transfer process could be intercepted. Wireless networks, for example, allow persons to connect to the Internet from anywhere inside a given radius, without the need for cable connections. However, this also allows perpetrators the same amount of access if adequate security measures are not implemented which will allow access to, *inter alia*, passwords, bank account information and other sensitive information. The criminalisation of the unlawful interception of data aims to protect the integrity, privacy and confidentiality of data within a computer device, a computer network, a database or an electronic communications network as well as data which is being sent to, over or from the aforementioned. The unlawful interception of data builds on the offence of illegal access, where further actions are taken by the perpetrator in order to acquire data unlawfully.

2.2.1.4.4 Section 86(1) of the ECT Act, No. 25 of 2002 criminalises the intentional interception of any data without authority or permission to do so. In terms of section 89(1) any person who

contravenes section 86(1), is liable to a fine or imprisonment for a period not exceeding twelve (12) months.

2.2.1.4.5 Section 2 of RICA furthermore prohibits -

(a) the interception of or attempted interception; or

(b) the authorisation or procurement of another person to intercept or attempt to intercept,

communications in the course of its occurrence or transmission, at any place in the Republic. Interception is defined in section 1 as the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the-

- monitoring of any such communication by means of a monitoring device;
- viewing, examination or inspection of the contents of any indirect communication; or
- diversion of any indirect communication from its intended destination to any other destination.

2.2.1.4.6 The offence solely relates to the interception of a direct communication (a communication between A and B, which takes place without technical means) and indirect communication (a communication between A and B, which takes place with technical means). In terms of section 49(1) of the RICA any person who intentionally intercepts or attempts to intercept, or authorises or procures any other person to intercept or attempt to intercept, at any place in the RSA, any communication in the course of its occurrence or transmission, is guilty of an offence. In terms of section 51(1)(b) of RICA, any person who is convicted of an offence referred to in section 49(1), is liable to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding ten (10) years. The offence in RICA is therefore not specifically applicable to hacking type of offences where access is obtained to a computer and information is downloaded. It must be noted that interception in terms of the RICA, relates solely to the interception of communications over an electronic communications system and will not cover the interception of communications stored on a computer (the so called hacking offences).

2.2.1.4.7 Article 3 of the Budapest Convention proposes the following offence:

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

2.2.1.4.8 The Convention does not define the concept of "interception".[4]

2.2.1.4.9 Article 29(2)(a) of the African Union (AU) Convention requires the criminalisation of the interception or attempted interception of computerized data fraudulently by technical means during non-public transmission to, from or within a computer system. Interception is also not defined.

2.2.1.4.10 Section 8 of the CW Model Law deals with the illegal interception of data. This section provides that a person who, intentionally without lawful excuse or justification, intercepts by technical means -

(a) any non-public transmission to, from or within a computer system; or

(b) electromagnetic emissions from a computer system that are carrying computer data;

commits an offence. Interception is not defined in the CW Model Law.

2.2.1.4.11 Section 6 of the HIPCAR[5] Model Law deals with this aspect. The following wording is proposed: A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, intercepts by technical means:

(a) any non-public transmission to, from or within a computer system; or

(b) electromagnetic emissions from a computer system,

commits an offence. Interception is defined in section 3(13) as including but not limited to the acquiring, viewing and capturing of any computer data communication whether by wire, wireless, electronic, optical, magnetic, oral, or other means, during transmission through the use of any technical device.

2.2.1.4.12 Section 6 of the Southern African Development Community (SADC) Model requires the criminalisation of interception. This provision provides that a person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification, intercepts by technical means -

(a) any non-public transmission to, from or within a computer system; or

(b) electromagnetic emissions from a computer system,

commits an offence. Section 6 further specifies that a country may require that the offence be committed with a dishonest intent, or in relation to a computer system that is connected to another computer system, or by circumventing protection measures implemented to prevent access to the content of non-public transmission. Section 3(16) defines interception as to includes but is not limited to the acquiring, viewing and capturing of any computer data communication whether by wire, wireless, electronic, optical, magnetic, oral, or other means, during transmission through the use of any technical device.

2.2.1.4.13 Section 5 of the International Telecommunication Union (ITU) Toolkit proposes in terms of section 5 that interception be criminalised. The text proposed provides as follows: Whoever intentionally and without authorisation pursuant to the rules of criminal procedure and any other laws of this country, intercepts, by technical means, transmissions of non-public computer data, content data, or traffic data, including electromagnetic emissions or signals from a computer, computer system, or network carrying or emitting such, to or from a computer, computer system and/or connected system, or network shall have committed a criminal offense. Interception is defined in section 1(k) as "the acquisition, viewing, capture, or copying of the contents or a portion thereof, of any communication, including content data, computer data, traffic data, and/or electronic emissions thereof, whether by wire, wireless, electronic, optical, magnetic, oral, or other means, during transmission through the use of any electronic, mechanical, optical, wave, electromechanical, or other device."

2.2.1.4.14 In the Philippines, section 4(2) of the Cybercrime Prevention Act of 2012 criminalises illegal interception, made by technical means without right of any non-public transmission of computer data to, from, or within a computer system including electromagnetic emissions from a computer system carrying such computer data. Section 3 (m) Interception refers to listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content of data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring.

2.2.1.4.15 In Singapore, section 6 of the Computer Misuse and Cybersecurity Act which deals with unauthorised use or interception of computer service, provides that any person who knowingly —

- secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service; or
- intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electromagnetic, acoustic, mechanical or other device,

is guilty of an offence. Section 2(1) defines "intercept" to mean, in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof. Section 2(1), further defines "electromagnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer.

2.2.1.4.16 In Canada, section 341.1(b) of the Criminal Code creates the offence of fraudulently and without colour of right, by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system. The section defines "electro-magnetic, acoustic, mechanical or other device means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing.

2.2.1.4.17 In Tanzania**,** section 6(1) of the Cybercrimes Act, 2015 criminalise illegal interception. This offence is worded as follows: A person shall not intentionally and unlawfully-

(a) intercept by technical means or by any other means-

(i) a non-public transmission to, from or within a computer system;

(ii) a non-public electromagnetic emission from a computer system;

(iii) a non-public computer system that is connected to another computer system; or

(b) circumvent the protection measures implemented to prevent access to the content of non-public transmission.

Section 3 defines "interception" in relation to a function of computer, includes acquiring, viewing, listening or recording any computer data communication through any other means of electronic or other means, during transmission through the use of any technical device.

2.2.1.4.18 In the United States of America 18 U.S.C. § 2511(1)(a), deals with interception (similar to RICA), and provides that except as otherwise specifically provided in this Chapter any person who intentionally intercepts, endeavours to intercept, or procures any other person to intercept or endeavour to intercept, any wire, oral, or electronic communication is guilty of an offence.[6]

2.2.1.5 It is the MNO's submission that the Bill does not specifically deal with what can be regarded as a *satisfactory exculpatory account of possession* and that especially where this is a new type of offence, it can lead to undue arrests and infringements of personal rights of individual(s). It is so that the courts would eventually rule on what should be regarded as *a satisfactory exculpatory account of possession*, but it is our submission that this should

also be addressed through *inter alia* training and in the Standard Operating Procedures issued to law enforcement officials and public sector incident response teams.

2.2.1.6 Spy hardware and software are commonly used in the commission of cyber offences. This type of hardware, as well as software may often be designed for legitimate and lawful purposes, but may subsequently be abused by criminals for unlawful purposes. Clause 4 aims to criminalise software or hardware tools which are unlawfully used in the commission of cybercrimes. The MNOs welcome the inclusion of this offence in the Bill, but wish to stress that the application of this offence should be covered in training to also bring into context that to establish the offence the intent to commit certain offences in the Bill must be present prior to any action being taken against a person(s).

2.2.1.7 Clauses 5 and 6 collectively deal with the unlawful interference with data or a computer program, as well as unlawful interference with a computer data storage medium or a computer system. It is our submission that these clauses recognise the importance of protecting the functioning, confidentiality, integrity and availability of data and computer programs and systems against unlawful interference e.g. as in the case of Denial of Service attacks.

2.2.1.8 Clause 7 criminalises the unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices, to commit an offence. The clause further criminalises *inter alia* the possession of passwords, access codes and similar data or devices, in regard to which there is a reasonable suspicion that it was acquired unlawfully and where the possessor is unable to give a satisfactory exculpatory account of such possession. Clause 7(2) again requires a person found in possession of such passwords, access codes and similar data or devices and where there is a reasonable suspicion that is was acquired unlawfully, to provide a *satisfactory exculpatory account of such possession*. See concerns raised in paragraph 2.2.1.5 *supra*.

2.2.1.9 The MNOs support the inclusion of Clause 7 as this type of offence in our experience leads to the commission of various other types of cyber offences.

2.2.2 Offences committed or facilitated by means of data, computer programs and computer systems

2.2.2.1 The MNOs support the inclusion of the offences of cyber fraud and cyber forgery and uttering respectively (Clauses 8 and 9) in the Bill. With the inclusion of Clause 8 in its current form and read with other applicable sections in the Bill, mobile network operators

in South Africa will now also be in a position to more effectively institute prosecutions for traditional telecommunications fraud such as International Revenue Share Fraud (IRSF), Wangiri fraud, etc.

2.2.2.2 The MNOs further submit that the in order to effectively prosecute the offence of phishing, whereas a false communication such as an email is drafted and sent out to victims to lure them to disclosing their personal information would be covered under Clause 9.

2.2.2.3 Clause 10 aims to criminalise cyber extortion and the MNOs support the inclusion of Clause 10 in the Bill.

2.2.3 Aggravated Offences

2.2.3.1 The MNOs recognise the need for the creation of aggravated offences as set out in Clause 11 and furthermore support the provisions in Clause 11 dealing with aggravated offences and the accompanying procedures prescribed under Clause 57 regarding the process of consultation to be followed with regards to declaring critical infrastructure.

2.2.4 Theft of Incorporeal

2.2.4.1 The MNOs welcome the inclusion of theft of an incorporeal under the common law crime of theft.

2.2.3 Penalties

2.2.3.1 The MNOs in principle support Clause 14 dealing with penalties for offences under Chapter 2, as well as those under Clause 15 dealing with competent verdicts, but wish to remark that the inclusion of the maximum amount of a fine might act as a further deterrent. It may also be considered to categorically state that proof of conduct criminalised in terms of Clause 12 shall attract sanctions of equal severity as the fines and imprisonment prescribed in Clause 14.

2.3 Ad Chapter 3: Malicious Communications

2.3.1 Clause 16 of the Bill aims to criminalise conduct where a data message is made available, broadcasted or distributed, by means of a computer system, a data message to a specific person, group of persons or the general public which incites the causing of any damage to any property belonging to, or violence against, a person or a group of persons. The MNOs wish to caution in that the implementation of this clause should be weighed up against an individual's right to e.g. freedom of speech and expression as enshrined in the Constitution.

2.3.2 According to Clause 17 any person who unlawfully and intentionally makes available, broadcasts or distributes by means of a computer system, a data message which is harmful, is guilty of an offence. A data message is considered harmful if the following conditions exists and if a reasonable person in possession of the same information and with regard to all the circumstances would regard the data message as harmful:

2.3.2.1 If it threatens a person with damage to any property belonging to, or violence against, that person, or damage to any property belonging to, or violence against, any member of the family or household of the person or any other person in a close relationship with the person;

2.3.2.2 it threatens a group of persons with damage to any property belonging to, or violence against, the group of persons or any identified person forming part of the group of persons or who is associated with the group of persons;

2.3.2.3 intimidates, encourages or harasses a person to harm himself or herself or any other person; or

2.3.2.4 is inherently false in nature and it is aimed at causing mental, psychological, physical or economic harm to a specific person or a group of persons.

2.3.3 Although the Protection of Harassment Act, 2011 was put on the Statute Book to comprehensively deal with harassment in the real and virtual world, many countries have recognised the seriousness of cyber harassment and have enacted specific laws which criminalise such communications. Cyber harassment is currently not recognised as a specific category of conduct in terms of the South African law and should be criminalised. The MNOs therefore welcome the inclusion of Clause 17 in the Bill.

2.3.4 In terms of Clause 18 any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message of an intimate image of an identifiable person knowing that the person depicted in the image did not give his

or her consent to the making available, broadcasting or distribution of the data message, is guilty of an offence. The MNOs support the inclusion of this offence in the Bill (as opposed to inclusion under the Harassment Act).

2.3.5 The MNOs support the provisions of Clause 19 that provide for an interim protection order pending finalisation of criminal proceedings, subject to the following:

2.3.5.1 In view of the fact that 'Social Media' or normal multi-media messaging services could be used to commit such offences, the provision of 19(1)(b) does not seem effective, since such messages become self-propagating, especially in reference to Clause 18 and even Clause 17. Unless the source from where such messages emanated before, also continue to emanate such messages and where the origination of such messages can in fact be established with proper certainty, this provision could easily only be applied punitively or in error and should be invoked with caution.

2.3.5.2 We also hereby express concern that instructions to "remove or disable access" could be regularly challenged where such instructions cannot be readily fulfilled. The fulfilment of such instructions can commonly only be determined after proper analysis of the manner by which incriminating messages are being conveyed. Where messages are conveyed by common IP packet transport, for instance, such transport may simultaneously carry multiple services including voice calls (using VoIP) for which further access to the telecommunications network cannot necessarily be allowed or disabled on a service-specific, selective basis. The "remove or disable access" can otherwise readily be fulfilled if a court order lists all services to be suspended, should the transport thereof be disabled.

2.3.5.3 A person or electronic communications service provider who contravenes a protection order is guilty of an offence. Provision is made for interim proceedings where the accused person can request the court to set aside or amend the protection order. The order of a court is subject to appeal or review.

2.3.5.4 Clause 19(b) only makes reference to a "computer system" and not computer storage medium or computer program which in our view should be included.

2.3.6 In terms of Clause 20, electronic communications service providers are compelled to assist a court (during proceedings in terms of Clause 19) to make available particulars of a person who distributed the malicious communications in order to ensure that the interim protection order can be served on him or her. The MNOs submit that this process would still be subject to the normal applicable court procedure. The practical implication hereof, especially where it relates to take down and further dissemination of messages is that it cannot always be lain

before the door of the electronic communications service provider, as for example is the case with the distribution of harmful messages on social media sites. Although an electronic communications service provider provides the means for transmission, electronic communications service provider such as Cell C, Telkom and Vodacom do not exercise control over the posting, storing and transmission of the actual content on these sites.

2.3.7 Clause 20 does however, make provision for us to supply affidavits stating that the data is not under our control and provision has been made to apply for an extension on the initial five (5) day period for the supply of information.

2.3.8 Clause 22 prescribes penalties which a court may impose in respect of malicious communications. It is the MNO's submission that in the instance of Clause 22(1) the penalty should be increased to a fine or to imprisonment for a period not exceeding five (5) years or to both a fine and such imprisonment.

2.4 Ad Chapter 4: Jurisdiction

2.4.1 Cell C supports the provisions relating to jurisdiction under Clause 23.

2.5 Ad Chapter 5: Powers to Investigate, Search and Access or Seize

2.5.1 Clause 24 provides for the issuing of Standard Operating Procedures which must be followed in the investigation of cyber offences or offences which have a cyber-element. The Standard Operating Procedures provides for the manner to deal with electronic evidence to maintain the integrity of evidence. As per the Memorandum this involves five principles namely -

2.5.1.1 legality;

2.5.1.2 no action taken should change data held on a computer or storage media which may subsequently be relied upon in court;

2.5.1.3 persons should be competent to access and be able to give evidence explaining the relevance and the implications of their actions;

2.5.1.4 an audit trail should be kept to enable an independent third party to examine those processes and arrive at the same result; and

2.5.1.5 any deviation from these principles should be explained.

2.5.2 The MNOs further recommend that a process of consultation with industry should be adopted when drafting the Standard Operating Procedures. These operating procedures could then also apply to the operations of the private sector computer security incident response teams to ensure uniformity of process and ease of presentation of evidence in court.

2.5.3 In terms of Clause 25, the Criminal Procedure Act, No. 51 of 1977 applies in addition to the provisions of this Chapter in so far that it is not inconsistent with the provisions of this Chapter. Currently cybercrimes are investigated in terms of the Criminal Procedure Act, No. 51 of 1977 and prosecuted in instances under the ECT Act, No. 25 of 2002 and Common Law).

2.5.4 The MNOs submit that the investigative procedures provided for in Chapter 2 of the Criminal Procedure Act are insufficient as they are object based and do not deal with the specialised procedures which are required to investigate cybercrimes, specifically when dealing with electronic evidence which is of an incorporeal nature and by its very nature fragile. Special procedures are further necessary to ensure the integrity of electronic evidence which is not specifically catered for in the Criminal Procedure Act and must now be addressed in the Bill.

2.5.5 Clause 27 provides that an article can only be searched for, accessed or seized by virtue of a search warrant issued by a judicial officer if it appears to the judicial officer, from information on oath or by way of affirmation that there are reasonable grounds for believing that an article is being used or is involved in the commission of an offence or is required as evidence at criminal proceedings.

2.5.6 It is furthermore our submission that the case law regarding the conduct of search and seizure operations in South African law is well-defined and would still be applicable in instances where the provisions of Clause 27 are invoked.

2.5.7 Exercise of search warrants although trite law must always be done with due regard to the rights of individuals and the businesses concerned and also where electronic communications service providers are concerned such as the MNOs, that interference with infrastructure and networks can disrupt communications for millions of South Africans.

2.5.8 Subject to any other law or obligation, the provisioning of Clause 27(1) must not be interpreted as to imply that the mere conveyance of a data message by an electronic communications service provider's computer system would imply that its computer system is involved in the commissioning of any category or class of offences, and thus an article to be searched for, accessed or seized.

2.5.9 The MNOs supports the provisions contained in Clause 28, 29, 30 and 31 respectively.

2.5.10 Clause 32 provides that an electronic communications service provider, financial institution and other persons, who are in control of data, a computer program, a computer data storage medium or a computer system must 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. Failure to comply can result in a conviction and a fine or imprisonment. The concern we wish to note is that no consideration is given to the reasonableness of the request. It is our submission that in instances where the request for assistances in the circumstances is viewed as unreasonable or can have a serious negative impact on the operations of an electronic communications service provider, this clause should make provision for some form of urgent relief. The same would apply in instances of Clause 33 (1).

2.5.11 The MNOs thus propose an amendment to Clause 32(1) to include that in the instance where an article which is under the control of an electronic communications service provider, is subject to a search authorised in terms of section 27(1), such search, access or seizure should be exercised in a way which must not disrupt the services performed by an electronic communications service provider.

2.5.12 In light of the fact that electronic communications service providers are mere conduits of information or data, the MNOs propose the inclusion of a "mere conduit clause", specifying that electronic communications service provider's shall not be criminally liable for criminal actions committed on its network unless they (electronic communications service provider's) have intentionally and unlawfully committed an offence under the Act."

2.5.13 The MNOs support the provisions of Clause 35, 36 and 37.

2.5.14 Clause 36 further regulates the instances where the disclosure of information will not amount to a contravention of this clause. The MNOs do, however, submit that the instances where disclosure is permitted should be addressed in more detail: where it pertains to police officials it can be addressed in standard operating procedures. We are hesitant to allow for information sharing by investigators that were designated to assist with searches where no legal remedies would be available for unlawful disclosure e.g. non-disclosure agreements are not in place. Where employees of an electronic communications service provider and financial institution would have obtained such information during the normal course of their duties (e.g. investigators) then there is no impediment to sharing according to normal business practice.

2.5.15 The MNOs caution that where cellular devices (if in scope) are targeted by search, access and seize operations, such actions must be approached with significant caution and oversight, since these devices commonly contain much personal information. "Investigator assistants"

that may commonly assist with 'search', 'access' and 'seize', could possibly fulfil a role of independent oversight. This should be addressed in training and in the Standard Operating Procedures and if these standard operating procedures are also publicised in regulations, it would enhance public confidence and transparency in the fairness of such procedures.

2.5.16 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 Chapter 5 of the Bill.

2.6 Clause 38 to 43: Interception of Indirect Communication, Obtaining of Real-time Communication-related Information and Archived Communication-related Information and matters incidental thereto

2.6.1 When enacted, the Regulation of Interception of Communications and Provision of Communication-related Information Act, No. 70 of 2002 ("RICA") dealt primarily with the interception of fixed line and mobile communications. Since the enactment of RICA, there has been a steady increase in cyber offences and subsequently an increase in the need for electronic evidence and the interception of communications that relate *inter alia* to such offences.

2.6.2 In terms of Clause 38 the interception of an indirect communication and obtaining of any real-time communication-related information on an ongoing basis, as it becomes available, must take place in terms of RICA. It also places additional requirements on electronic communications service providers that are not required to be interceptable or to store communication-related information as per the provisions in Government Notice No. 1325 of 2005.

2.6.3 Insofar as our obligations under RICA, the MNOs can in instances have obligations both as telecommunications service providers and internet service providers, as we all operate in multiple service/technology segments that are not so clearly distinguished and separated as what RICA might suggest. (This is *inter alia* due to the advent of technologies such as 3G, LTE, LTE Advanced and Fibre.)

2.6.4 It is furthermore our understanding that where directions are served under RICA nothing in the Bill now states that directions will be served differently as per our existing processes and prescripts and that any *preservation* or *disclosure* directions that fall outside the ambit of RICA will be handled and served completely separately. The MNOs would agree to such an approach as it would not compromise security of the RICA processes. We would further

recommend that similar processes and prescripts be put in place when dealing with any preservation or disclosure directions.

2.6.5 In our understanding of the requirements of the Bill there would thus be a requirement to not only determine WHEN a person was on the Internet, but that the Bill now actually imposes an onerous obligations on all to determine in WHAT activities such a person engaged. The Bill accordingly wishes to obtain sight of a person's activities on the Internet without the collection of metadata or the analysis of the contents of indirection communications where such information could previously be obtained and placed at the disposal of investigators through interception measures applied in terms of RICA.

2.6.6 The MNOs wish to note that to date no additional study has been performed to determine what the implications both operationally and financially would be of such requests for preservation and expedited preservation of data as envisaged under Clauses 39 and 40. It is our submission that telecommunications service providers/electronic communications service providers already carry a heavy financial burden in enforcing the provisions of RICA in terms of the provision of real-time and archived communication and to impose additional requirements without a full impact assessment would be imprudent.

2.6.7 The MNOs furthermore submit that there is no safeguard against duplicate costs due to obligations under RICA and the Bill that may serve the exact same purpose (and deliver similar results).

2.6.8 Clause 38(3)(b)(v), 46(6) and 46(7): Revised role of the Designated Judge

2.6.8.1 RICA contains prescripts that confine the role of the Designated Judge to solely effect and oversee the objectives of that Act. In context of Clause 38(3) and Clause 46(6), the Designated Judge is now additionally commissioned to further the objectives of *preservation of data*, *evidence* or *other article*, *seizure of data*, the e*xpedited disclosure of traffic data* and *data obtained from interception and preservation* as per prescripts related to cybercrime. From such prescripts the following difficulties arise:

a. An interception order in terms of RICA commonly holds a higher security classification than requests for information concerning more common criminality. Should orders be issued that otherwise instruct the *preservation* or *seizure'* of data (information) it must be ensured that no higher security classification than "confidential" is applied to enable staff receiving such orders to forward orders to

other departments and staff for execution thereof, without fear of prosecution (including charges of treason where “Top Secret” orders are disclosed).

b. The reading of the prescripts per Clause 46(7)(b) pertaining to the recipient electronic communications service provider in context of the obligations per Clause 46(6) that include obligations to intercept indirect communications seem to impose a new obligation on electronic communications service providers to retain the results of lawful interception (for preservation purposes). Currently, there is no prescript in the RICA Act for such service providers to store the results of any interception of any indirect communications for later disclosure – results of interception are currently only delivered in real-time to the authorised destination. Should RICA be augmented in this manner, technical prescripts must be added to that Act or its associated Directives, to this effect and we submit that this should be in consultation with electronic communications service providers as this will have a huge operational and financial impact on such institutions.

c. Prescripts of 46(7)(b) makes reference to *persons*, *electronic communications service provider* and *financial institution* who can be targeted by orders from the Designated Judge, where such orders may include instructions to *intercept*. However, only *electronic communications service providers* must currently comply with RICA and give effect to directions from the Designated Judge and other recipients would not have the requisite or equivalent facilities.

d. In general, it would be appropriate to clarify exactly and to what extent, the contents of directions may deviate from the prescripts of RICA where such directions emanate from the Office of the Designated Judge in terms of further obligations enforced by these prescripts. This is to ensure the timeous and uncontested execution thereof.

e. In general, it would also be appropriate to separately clarify exactly what further powers and obligations are delegated to the Designated Judge in cases of cybercrime, to ensure that there is no misunderstanding or unnecessary contention about what instructions may henceforth emanate from his or her office.

2.6.9 Clauses 39 through 42: *Data* and *Evidence*

2.6.9.1 It must be appreciated that telecommunications service providers (or electronic communications service providers under the Bill) currently have precise knowledge of the type of real-time or archived information that may be requested under direction from the

Designated Judge and under RICA. Furthermore, these service providers understand precisely what alternative information must be provided in real-time while interception orders are in progress, how such information must be constructed and conveyed per predefined and ETSI-standardised ASN.1 delivery formats. The manner in which such interception orders must be executed for fixed line and mobile services, voice and data services, real-time and messaging services is also well-defined and standardised. Such targeted interception measures are also applied very discriminatively to ensure that only the indirect communications of specific individuals is obtained in a highly selective manner.

2.6.9.2 It is the MNO's submission that this Bill gives no specific direction or foresight on any further data or evidence that must now commonly be preserved or would commonly be required under direction of police officials, magistrates or judges or the designated judge. Only "traffic data" is understood to reference "billing information" that may also be requested under RICA.

2.6.9.3 It must accordingly be understood that it is a daunting prospect to be served with any order to obtain and preserve *data* or *evidence* to allow for criminal proceedings supported by expert testimony in cases of the commission of cybercrime(s) where these orders should apparently be complied with on an ad-hoc and highly disruptive basis. Each order might require a unique or customised approach or solution that may not be immediately evident or may be costly or complex to implement. Some orders might in any event not be feasible and could be contested.

2.6.9.4 A *disclosure of data direction* is expected to convey further instructions to refine the data to be disclosed (this is presumed to include the analysis and filtering of data previously preserved, by order) and the format in which such data must be provided (*ad* Clause 42(2)(d))(this is presumed to further prescribe the preparation and pre-processing of data prior to submission for further forensic analysis, in a specific format). It cannot be assumed that such data processing/formatting facilities are readily available or can otherwise be readily acquired or operated with little skill by electronic communications service providers.

2.6.9.5 In conclusion the establishment of Standard Operating Procedures is crucial to give better guidance on the manner in which orders must be complied with. THE MNOs further submit that the successful implementation of the Bill will largely rely on the preparation work that is prescribed by the Bill: in terms of structures that must be established, consultations that must be done and agreed to, training that must be finalised, etc.

2.6.10 Clauses 39 and 40: Expedited Preservation Orders for Data/Evidence

2.6.10.1 In reference to such obligations, the following concerns are hereby raised:

a. Where data preservation orders are received that carry a “Top Secret” classification such orders can only be dealt with by individuals that have the appropriate clearance. The MNOs are concerned that we might receive preservation orders where the information requested would necessitate the involvement of individuals that do not have the prerequisite clearance levels.

b. The MNOs wish to caution that when receiving preservation orders as envisaged in the Bill, electronic communications service providers might be placed in the situation that they cannot comply in full or partially with such orders because of *inter alia* inadequate storage capacity, hardware and software requirements.

c. A direction for preservation of data would imply ownership and application of equipment that should be classified as "listed equipment" in terms of Clause 44 of RICA and where such equipment may only be in possession of the recipient of the direction in terms of a certificate issued under Clause 46(2)(b) of RICA where the ownership and use of such "listed equipment" can only be ratified under motivation of reasonable necessity. (Note that such certification excludes equipment that must be owned and operated to otherwise give effect to directions for the interception of indirect communications in terms of RICA). By implication, RICA places restraint on the ownership and daily operation of equipment that would place means at the disposal of electronic communications service providers to readily give effect to directions to obtain and filter data (to limit such data on grounds of *in respect of a customer*). From an operational perspective, grounds for reasonable necessity should be constrained to the necessity to merely maintain the integrity and performance of a telecommunications network and to otherwise "register" information for "commercial purposes" (i.e. billing). Accordingly, it is inconceivable to deduce that electronic communications service providers would commonly and legally have *certifiable* equipment in their possession that is sufficiently intrusive on their customer's constitutional right to privacy and also amply sophisticated to simultaneously satisfy these preservation orders.

2.6.10.2 In view of the submission above, it would be pertinent to constrain expectations on what data should be reasonably preserved. The MNOs hereby express concern about the legal

workload and costs to contest regular preservation orders on grounds of unreasonable expectations or substantive technical limitations.

2.6.11 Clause 42: Disclosure of Data Only

2.6.11.1 Clause 42 contains prescripts for *disclosure of data* directions (from (42(1)(b)(ii) onwards) whereas this clause should also apparently cover *preservation of evidence* (see 42(1)(a)). It remains uncertain how and under what conditions and authority, custody of *preserved evidence* (or *article*) must be transferred to criminal investigators. Such evidence could be a whole computer system that may also be of significant monetary value.

2.7 Ad Chapter 6: Mutual Assistance

2.7.1 Clause 44 provides that the provisions of sections 46 to 49 apply in addition to Chapter 2 of the International Co-operation in Criminal Matters Act, 1996, and relate, unless specified otherwise, to the preservation of evidence pending a request in terms of section 2 or 7 of the International Co-operation in Criminal Matters Act, 1996.

2.7.2 In terms of Clause 44 The National Commissioner may, on such conditions regarding confidentiality and limitation of use as he or she may determine and after obtaining the written approval of the National Director of Public Prosecutions as contemplated in subsection (2), forward any information obtained during any investigation to a law enforcement agency of a foreign State under certain conditions. The South African Police Service may similarly receive any information from a foreign state, subject to such conditions regarding confidentiality and limitation of use as may be agreed upon, which will assist the South African Police Service in the investigation of a cybercrime or offences contemplated in clause 16, 17 or 18.

2.7.3 Although Clause 47 imposes obligations on a person, electronic communications service provider or financial institution to comply with an order of the designated judge issued in terms of Clause 46 there is provision for a process to apply to the Designated Judge for an amendment or the cancellation of the order concerned on the ground that he, she or it cannot timeously or in a reasonable fashion, comply with the order.

2.7.4 Clause 48 further provides that any traffic data which is made available on an expedited basis, in terms of an order in terms of clause 46, must be provided to the 24/7 Point of Contact for submission to a foreign State. It is unclear who is to provide the data to the 24/7 Point of

Contact and if this Clause envisages a deviation from the processes that we as MNOs have in place in terms of RICA. Would the information be handed to the designated police official that would in turn provide it to the 24/7 Point of Contact? The MNOs would therefore request a clarification on what the implication of this clause would be.

2.8 Ad Chapter 7: 24/7 Point of Contact

2.8.1 Cell C supports and commends the inclusion of Clause 50 in the Bill, which provides for the establishment and functions of the 24/7 Point of Contact as part of the South African Police Service.

2.9 Ad Chapter 8: Evidence

2.9.1 As stated in paragraph 1.1.6 *supra* the Bill should make reference to the findings of the Law Reform Commission regarding the submission of electronic evidence.

2.10 Ad chapter 9: Obligations of Electronic Communications Service Providers and Financial Institutions

2.10.1 In terms of Clause 52 an electronic communications service provider or financial institution that is aware or becomes aware that its computer system is involved in the commission of any category or class of offences provided for in Chapter 2 and which is determined in terms of subsection (2), must:

2.10.1.1 without undue delay and, where feasible, not later than 72 hours after having become aware of the offence, report the offence in the prescribed form and manner to the South African Police Service; and

2.10.1.2 preserve any information which may be of assistance to the law enforcement agencies in investigating the offence.

2.10.2 It is the MNO's understanding there is however, no obligation on electronic communications service providers and financial institutions to report cybercrimes and to preserve evidence of

cybercrimes on their systems. Clause 52(4) provides that subject to any other law or obligation, the provisions of subsection (1) must not be interpreted as to impose obligations on an electronic communications service provider or financial institution to:

2.10.2.1 monitor the data which the electronic communications service provider or financial institution transmits or stores; or

2.10.2.2 actively seek facts or circumstances indicating any unlawful activity.

2.10.3 The MNOs do however, submit that subject to any other law or obligation, the provisioning of subsection (1) must not be interpreted as to imply that the mere conveyance of a data message by an electronic communications service provider's computer system would imply that its computer system is involved in the commissioning of any category or class of offences provided for in Chapter 2.

2.11 Ad Chapter 10: Structures to Deal with Cybersecurity

2.11.1 The Bill foresees the establishment of a 24/7 Point of Contact (under the SAPS), a Cyber Response Committee and a computer security incident response team (under State security) and a Cybersecurity Hub (under the Department of Telecommunications and Postal Services) whereas the latter must serve as mediation point and promote the establishment of sectoral nodal points and sectoral computer security incident response team. The MNOs submit that there is no clarity as to which Organ of State ultimately holds supreme authority to ensure that these entities all operate and interact seamlessly and that the overall objectives of the Bill are achieved.

2.11.2 Although we as MNOs in essence support the structures that are to deal with Cybersecurity it is not clear yet what the incoming obligations and likely costs would be that would be associated with the setup of nodal points as no reference is made to such a discussion or consultation process under Clause 55(1)(a). The only reference to cost is that in Clause 55 (4) which states that a particular sector is responsible for the establishment and operating costs of a nodal point established in terms of subsections (2) or (3). It is our submission that there should be a proper cost and impact assessment done prior to implementation of such a responsibility.

2.11.3 Clause 56 deals with information sharing and states that the Cabinet member responsible for the Administration of Justice must make regulations to regulate information sharing, for

purposes of this Chapter, regarding cybersecurity incidents and the detection, prevention, investigation or mitigation of cybercrime. In dealing with the cyber security structures described in chapter 10 we would be concerned if there was any attempt (directly or indirectly) to force mandatory information sharing (notwithstanding the obligations in chapter 9) without a proper consultation process. The exchange of information should only take place in circles of trust where we can verify that information is protected, used appropriately, proportionate to the threat and reciprocated. The MNOs would therefore recommend that the regulations be made at least after a thorough process of consultation with the relevant parties.

2.12 Ad Chapter 11: Critical Information Infrastructure Protection

2.12.1 National Critical Information Infrastructure is defined in the National Cybersecurity Policy Framework for South Africa, Government Gazette No. 39475 of 4 December 2015 as all ICT systems, data systems, data bases, networks (including people, buildings, facilities and processes), that are fundamental to the effective operation of the Republic.

2.12.2 International Definitions of Critical Information Infrastructure

2.12.2.1 The African Union Defines Critical Cyber/ICT Infrastructure as the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability and for the sustainability and restoration of critical cyberspace.[7]

2.12.2.2 The Organisation for Economic Co-operation and Development (OECD) defines critical information infrastructures in a manner that should be understood as referring to those interconnected information systems and networks, the disruption or destruction of which would have serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy.[8]

2.12.2.3 The Global Forum on Cyber Expertise (GFCE-Meridian) states that critical information infrastructure are those interconnected information and communication infrastructures which are essential for the maintenance of vital societal functions (health, safety, security, economic or social well-being of people) - the disruption or destruction of which would have serious consequence.[9]

2.12.3 Clause 57 deals with the protection of critical information infrastructures. This clause does provide for an extensive consultation process with the various parties involved before an

information infrastructure may be declared a critical information infrastructure which is commendable.

2.12.4 As per the Memorandum, critical information infrastructures are not adequately protected. Legislation exists for the protection of physical structures, which cannot be used to protect computer systems. The ECT Act, 2002 furthermore, narrowly caters only for the protection of databases and not for other information infrastructures which need to be protected.

2.12.5 No provision is currently made for the implementation of minimum security standards which are necessary to protect critical information infrastructures or to monitor compliance with such standards. Furthermore, the Bill differs from the provisions in the ECT Act, 2002 which spoke to critical databases[10] housing essential data. It is our submission that the provisions in the Bill are broad when referring to information infrastructure and the Bill speaks vaguely to infrastructure pertaining to a potential "disruption of an essential service," or "destabilisation of the economy of the Republic".

2.12.6 The MNOs submits that it might be prudent to look at extending the definition to also specifically refer to critical information infrastructure, which includes any critical database and the data housed thereon. The definition must also not lose sight of the processes used to control, enable and protect the data contained in such critical databases.

2.12.7 In terms of Section 57(7), the owner or controller may dispute the decision and lodge the dispute within thirty (30) days after 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.

2.12.8 The MNOs submit that when the dispute resolution regulations are issued, they should cater for the length of the arbitration process, should a dispute be lodged.

2.12.9 The MNOs accordingly recommend 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.

2.12.10 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 two (2) years' imprisonment or a fine or both.

2.12.11 The MNOs submit that in order to give effect to the directives issues in terms of Section 57 such an assessment be done to measure the financial impact the cost of compliance will have on electronic communications service providers. The MNOs further submit that it must also

be borne in mind that in some instances electronic communications service providers do not own the (physical) network infrastructure e.g. base stations used by the network.

2.12.12 Clause 58 provides for the auditing of critical information infrastructures to ensure compliance with a directive which is issued by the Cabinet member responsible for State security in terms of clause 57. Section 57 of the ECT Act stated that the Director-General could cause audits to be performed at a critical database administrator to evaluate compliance with the provisions of this Chapter. These audits were to be performed by either the cyber inspector or an independent auditor. It is the MNOs submission that requiring that these audits be performed at the cost of the owner or person in control of the critical information infrastructure must be reviewed.

2.12.13 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.

2.12.14 The MNOs shall otherwise welcome a revision of prescribed standards on the protection of critical information where such standards should then also be maintained to ensure best practices continue to prevail, as technology evolves.

2.13 Ad Chapter 12: Agreements with Foreign States

2.13.1 It is the MNOs submission that current procedures for mutual assistance between South Africa and foreign countries in the investigation of cybercrimes do not effectively take into account the transient nature of electronic evidence and the need to act expeditiously. The resultant effect is that essential evidence is lost. Various other countries enacted legislation to provide for urgent action to preserve information and to provide expeditious assistance to identify the origin of communications involved in a cybercrime. The MNOs support the provisions under Chapter 12 in the Bill.

2.13.2 The MNOs otherwise assume that the 24/7 Point of Contact will be commissioned to provide expert guidance should evidence be required in electronic format in a manner that will ensure that such evidence should not be rejected in a court of the Foreign State on grounds of misalignment with local prescripts to preserve and ensure the integrity of such electronic evidence.

2.14 Ad Chapter 13: General Provisions

2.14.1 In terms of clause 60, the NDPP is obliged to keep statistics of the number of prosecutions instituted in terms of Chapter 2 or clause 16, 17 or 18 of the Bill, the outcome of such prosecution and any other information relating to such prosecutions, which is determined by the Cabinet member responsible for the administration of justice. These statistics must be included in the report of the NDPP, referred to in section 22(4)(*g*) of the National Prosecuting Authority Act, 1998, and on the written request of the Chairperson of the CRC be made available to the CRC.

2.14.2 The MNOs do however, recommend that the obligation on the South African Police Service (SAPS) to report on these same statistics be reviewed to ensure accurate reporting of these crimes and not only on those that actually make it to court. This would also contribute towards accurate reporting on how effective investigations into these type of offences are and what percentage of cases actually result in prosecutions.

- END -

---

1 ETS No. 185

2 Seger, Alexander Identity theft and the Convention on Cybercrime UNISPAC Conference on the Evolving Challenge of Identity-related Crime (Courmayeur, Italy, 30 November – 2 December 2007)

3 European Commission Directorate General for Home Affairs Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft 11 December 2012

4 (See in general paragraph 51 to 59 of the Explanatory Report to the Budapest Convention. - The notion that a “radio” may encompass a “computer system” cannot be supported (Paragraph 56)). In terms of paragraph 53 of the Explanatory Memorandum, interception by "technical means" is a restrictive qualification to avoid over-criminalisation. Paragraph 54, explains that the requirement of a “non-public” transmission further restricts the ambit of Article 3).

5 The HIPCAR Project was conceived by the ITU, the Caribbean Community (CARICOM) Secretariat and the Caribbean Telecommunication union (CTU) in response to requests from CARICOM States and other ICT stakeholders who saw the need for a more unified approach to the subject.

6 See also: Section 12 of the Prevention of Electronic Crimes Act, 2015 of Pakistan; Botswana section 9; Section 12 Nigeria; Section 202(b) St GB of Germany; Article 8 of the Computer Crimes Act of Sri Lanka; Art.285 of Criminal Law of the People’s Republic of China; India - Information Technology Act of 2000, Section 43(b) and Section 66; United Kingdom – Section 1 of the Regulation of Investigatory Powers Act 2000; Canada - Criminal Code, Interception of Communications, Sections 183-196 and Unauthorized

Use of Computer, Section 342.1; Article 139c of Netherlands Wetboek van Strafrecht; Australia section 7 of the TIA.

7 http://pages.au.int/sites/default/files/en_AU%20Convention%20on%20CyberSecurity%20Pers%20Data%20Protec%20AUCyC%20adopted%20Malabo.pdf

8 http://www.oecd.org/sti/40825404.pdf

9 The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers, November 2016

10 In terms of the ECT Act "critical data" means data that is declared by the Minister in terms of section 53 to be of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens; "critical database" means a collection of critical data in electronic form from where it may be accessed, reproduced or extracted.