# [Joint Industry Submission on the Cybercrimes and Related Matters Bill](https://www.sacomforum.org.za/?p=2632)

March 23, 2015

**MTN, VODACOM, CELL C, TELKOM AND NEOTEL JOINT INDUSTRY SUBMISSION ON THE CYBERCRIMES AND RELATED MATTERS BILL**

1 Introduction

MTN, Vodacom, Cell C, Telkom and Neotel (hereinafter referred to as the “ICT ECSPs”) would like to thank the Department of Justice and Constitutional Development (“DoJ”) for the opportunity and invitation to comment on the draft Cybercrimes and Related Matters Bill of January 2015 (“the Bill).

This joint submission seeks to provide the DoJ with the views and proposals made by the ICT ECSPs before the Bill is presented to Cabinet.

2. General Comments

2.1 National Cybersecurity Policy Framework

On 7 March 2012 the National Assembly approved the publication of the draft National Cybersecurity Policy Framework (“draft NCPF”) which was aimed at promoting a culture of cybersecurity and provides a holistic approach pertaining to the promotion of cybersecurity measures by all role players in relation to cybersecurity threats. The draft NCPF was subsequently followed by the drafting of the Bill that was circulated by the DoJ in October 2014. It is expected that the Bill will culminate into legislation governing cybercrime in South Africa.

The ICT ECSPs are concerned that the DoJ is in the process of finalising the Bill without clarifying government’s approach towards cybersecurity issues. This makes it difficult to contextualise the Bill against the challenges that it intends to address. In this regard, we request that the DoJ finalise the NCPF and advice on the extent to which it considered the draft NCPF when drafting the Bill.

2.2 The Current legislative Framework

*2.2.1 Process of criminalization*

There is no indication that an extension of the common law offences or an amendment to the statutory offences is likely. This possibility is dependent on the level of appreciation of the dangers of the relevant activities among the judiciary. It is further dependent upon the willingness of the investigating and prosecuting authorities to prepare a case for prosecution in the hope of convincing a court that a common law offence should be extended to apply to a set of circumstances to which it did not apply hitherto. This seems to indicate that the option of introducing new offences by way of legislation should be seriously considered, however, caution should be applied to ensure that any possible duplication is appropriately dealt with, and that legal and regulatory certainty exists.

*2.2.2 Structures to deal with Cyber Security*

The precise nature of the support that is to be rendered by the relevant structures and the roles and responsibilities for each structure needs to be clearly defined. As it currently stands, the Bill introduces a host of new structures, but it is not clear how these structures will interact with each other, with current existing structures (example SAPS or the newly formed Information Regulator) or with the ICT ECSPs. Failure to adequately detail the precise nature of the support and the interaction between structures may result in confusion, duplication of efforts and regulatory uncertainty.

*2.2.3 Duplications in respect of other legal instruments*

Upon perusal of the Bill, the ICT ECSPs identified that there are provisions, crimes and definitions in the Bill that are addressed in other pieces of legislation. The ICT ECSPs note that although there is duplication with other pieces of legislation, the Schedule attached to the Bill does not include references to these pieces of legislation and it is not clear whether such legislation will be amended and/or repealed. Furthermore, existing definitions from other legislation and the common law (as discussed above) have not been incorporated in the Bill.

While we have noted the DoJ’s requirements to have all cybercrimes regulated in a single bill, the current drafting may cause regulatory uncertainty, confusion and duplication. Below are some examples of the duplications that are of concern:

1. Section 2, Personal information related offences- All personal information related offences will be regulated by the Protection of Personal Information Act (No. 4 of 2013) (“POPI”). Although POPI is not in effect yet, it has been promulgated and it is expected that it will come into effect in due course. Personal Information is defined in great detail in POPI.[[1]](#footnote-1)

The proposed definition of personal information in the Bill is narrow and the proposed offence does not cover the extent of the protection that will be provided in terms of POPI. It is further unclear how the Bill will interact with the provisions of POPI, particularly relating to the protection of data subjects[[2]](#footnote-2) which will include victims and potential perpetrators;

2. Section 4, Unlawful interception of data – It is not clear how this offence interacts with the Regulation of Interception of Communications and Provision of Communication-Related Information Act (No. 70 of 2002) **(“RICA Act”)** which deals with the interception of communications. In particular, section 49 of the RICA Act makes it an offence to unlawfully intercept communications. Detailed submissions on the RICA Act are made further in this joint submission;

3. Sections 10 and 11, Computer related fraud; and computer related forgery and uttering. The ICT ECSPs note that similar crimes as currently described in sections 86 and 87 of the Electronic Communications and Transactions Act (No. 25 of 2002**) (“ECTA”).** While we note that these sections will be repealed by the Bill, it is our submission that the DoJ should ensure that the new proposed sections 10, 11, 12 and 13 are sufficient to adequately deal with all crimes of this nature to ensure that a legal lacuna is not created when the sections of ECTA are repealed;

4. Sections 12, 13 and 15, Computer related appropriation; computer related extortion; and computer related espionage – These provisions appear to be very similar to the common law crimes of theft, extortion and high treason / sedition. Due to the similarity and overlap with the common law crimes, the current drafting could possibly replace or impact on the common law crimes theft, extortion and high treason / sedition;

5. Section14-The Protection of State Information Bill had sections that were to introduce information classification in the interest of national security. We therefore believe that due to the fact that this Bill has provisions that relate to classification levels, the ICT ECSPs would need to understand the alignment and interaction between the two bills.

6. Section15 Computer related terrorist activity and related offences- It is not clear how this provision will interact with the Prevention of Organised Crime Act (No. 121 of 1998), which already has provisions relating to property used to commit terrorist activities;

7. Section 16 Prohibition on dissemination of racist and xenophobic material- Chapter 3 of the Film and Publications Act (No. 65 of 1996) **(“FPA”)** provides that it is an offence to broadcast or distribute hatred founded on any identifiable group characteristic which constitutes incitement to cause harm;

8. Section 17, Prohibition on incitement of violence- Chapter 3 of the FPA provides that it is an offence to broadcast/publish a publication on hatred based on any identifiable group characteristic which constitutes incitement to cause harm. The ICT ECSPs would like to understand the alignment and interaction between the FPA and the provisions of the bill dealing with the incitement of violence;

9. Section 18, Prohibited financial services- The ICT ECSPs submits that this is sufficiently addressed in the Financial Intelligence Centre Act (No. 38 of 2001);

10. Section 19, Infringement of copyright- The infringement of copyright is adequately addressed in the Copyright Act (No. 98 of 1978). In particular section 27 of the Copyright Act has various offences relating to the selling, hiring, exhibiting, importing, and distributing of copyrighted work;

11. Section 20, Child pornography –The Sexual Offences and Related Matters Act (no. 32 of 2007, as amended) addresses all child pornography related offences and adequately defines child pornography, sexual violation and sexual penetration. Chapter four, part two and three of the Sexual Offences and Related Matters Act specifically discuss child pornography. Detailed submissions in respect of this section are made later on in this joint submission;

12. Section 21, Harbouring or concealing person who commits offence- This section is addressed in the Criminal Procedure Act (No. 51 of 1997). The Criminal Procedure Act makes reference to various unlawful acts which can be committed by either the offender or an accomplice. Furthermore, the current wording in the Bill is too broad and may have unintentional consequences and if not removed, should be narrowed significantly to address the actual intention of the offence; and

13. Sections 22 and 23, Attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instructing, commanding, or procuring to commit offence; Aggravating circumstances when an offence is committed in concert with other persons - These sections are addressed in the Criminal Procedure Act. The Criminal Procedure Act makes reference to various unlawful acts which can be committed by either the offender or an accomplice.

2.3 The term “Cyber Security”

The ICT ECSPs note that various references to cyber security appear in the Bill. The ICT ECSPs submit that the Bill is intended to deal with cyber related crimes and not cyber security in general as they are two different concepts. Accordingly, ICT ECSPs request clarity on whether the Bill will address both concepts and if so, both concepts should be adequately defined in the Bill.

2.4 Structures dealing with Cyber crime

Chapter 6 of the Bill sets out various structures and teams to govern interaction and collaboration between government, private sector and civil society in an effort to deal with cybercrimes and related matters. The Bill however fails to explain how these structures relate to each other nor does it clarify their specific roles and responsibilities. Failure to clarify the relationship between these various structures is likely to lead to duplication of responsibilities and will defeat the rationale behind their creation.

The ICT ECSPs submit that the Bill should create a single structure to deal with cybercrimes and related matters. The aforesaid structure should be well capacitated and act as a single point of contact on all cybercrimes and related matters, coordinate cybersecurity responses, establish guidelines and best practices for the country.

The creation of a single structure cannot be effective in isolation. The creation or strengthening of the aforesaid structure should be part of an effective cybercrime strategy driven at a national level by the Cabinet Minister responsible for State Security. The strategy should aim at developing mechanisms that ensures proactive and coordinated national responses to cyber threats and incidents including prevention of cybercrimes. Cooperation with the private sector is also essential not only in terms of securing electronic evidence but also for prevention, threat assessments, investigations and training.

3. Specific Comments

3.1 Definitions

Cybercrime

Following from our general comments on the term “Cyber Security” the DoJ does not have an official definition of cybercrime that distinguishes it from the common law definition. This makes it difficult to distinguish cybercrime from other forms of cyber threats. We believe that in order to ensure certainty and consistency in the application of the term the Bill should contain an appropriate definition of cybercrime.

As the starting point the DoJ should seek guidance from the NCPF which defines cybercrime as “illegal acts, the commission of which involves the use of information communication technologies”. This definition, however, does not go far enough since it fails to take into account the nature of cybercrime and its salient features. We are of the view that when defining cybercrime its characteristics should be kept in mind since it differs in material respect from traditional crimes and present investigative challenges, viz.

* It is committed within the cyber space environment;
* The investigative agency needs the assistance of the ICT ECSPs to investigate the crime. This is a complete contrast to the existing modus operandi where the law enforcement agency is solely responsible for the investigation of the crime and can solicit the assistance of any person who is relevant to the investigation;
* In many instances the perpetrator is not located within the borders of the Republic but the effect of the crime is felt in the country.

In light of the above The ICT ECSPs propose the following definition:

**“Cybercrime”** means “an array of illegal activities committed within an electronic medium or cyberspace and which is committed within or having an effect in the Republic”.

3.2 Child Pornography, Section 20(6)

Section 20(6) of the Bill includes a provision on Child Pornography, which provision provides that any electronic communication service provider who intentionally and unlawfully-

a) Makes available, distributes or broadcasts;

b) Causes to be made available , broadcast or distributed;

c) Assists in making available, broadcast or distribute,

child pornography through a computer network or electronic communications network, is guilty of an offence.

According to the South Africa Concise Oxford Dictionary the word “intentionally/intention” is defined as “the action or fact of intending”. In criminal law intent or mens rea refers to the mental intention or the defendant’s state of mind at the time of committing an offence and must be proved prior to convicting a defendant of a crime). The ICT ECSPs are in the business of transporting content over its network and therefore there is an intention to transport content between content providers and our subscribers. However, if the location (i.e. the URL) of child pornography content that is made available on the internet has been made known to us, we will block such content from being accessed by our subscribers. The ICT ECSPs therefore submit that section 20(6) should be amended to cater for the current process that we are utilising to block child pornography content from being accessed by our subscribers over the internet. Our proposed amendments are as follows:

“any electronic communication service provider who does not action a valid take-down notice from a Child Pornography Reporting Party and Intentionally and unlawfully-

a) Makes available, distributes or broadcasts;

b) Causes to be made available , broadcast or distributed;

c) Assists in making available, broadcast or distribute,

child pornography through a computer network or electronic communications network, is guilty of an offence.

In addition, the term “Child Pornography Reporting Party” must be defined to mean “the Internet Watch Organisation or similar organisation” The term “take-down notice” should also be defined and mean “a notice to block access to a specific URL that is the address of website containing child pornography content.”

The ICT ECSPs submit that such amendments are necessary because the above mentioned process has not been prescribed in legislation such as the FPA.

The ICT ECSPs are especially concerned that section 20(6) in the Bill can be interpreted to mean that the providers may have to identify Child Pornography content through active interception of electronic communications and once the content has been identified, a mechanism needs to be implemented to prevent the end-user from viewing or accessing the content in order to comply with section 20(6)(c). If this interpretation is accepted as correct, then the ICT ECSPs would be in violation of the RICA Act which prohibits the interception or inspection of communication related information without the proper consent from the end-user. To this end DoJ should appreciate that we can only identify the type of service that is accessed and not inspect what is contained in that content.

The ICT ECSPs submit that it will not be in position to identify when such content (identified through active interception) is carried over its network as technologies such as deep packet inspection will need to be implemented, which will have the following disadvantages:

1. Such technologies will result in network performance issues for the ICT ECSPs, licensed in terms of the Electronic Communications Act, (No 36 of 2005) (“ECA”) and such providers may not be in position to comply with End-User and Subscriber Service Charter Regulation (Government Gazette: 32431 of 24 July 2009). This regulation, published by the Independent Communications Authority of South Africa (“ICASA”) prescribes the network performance thresholds for licensees who operate an electronic communication network as defined in the ECA.

2. The implementation of such technologies will have a significant cost impact to the ICT ECSPs and such costs would need to be recovered. The ICT ECSPs may be forced to recover such additional costs from the consumers, which goes against government’s policy objective to reduce the cost to communicate.

The ICT ECSPs therefore submits that our proposed amendment as specified above will also ensure that such an interpretation or the obligation to unlawfully intercept electronic communication is avoided.

3.3 Article to be accessed or seized under search warrant, Section 29

Section 29 (2)(e) states: “A search warrant issued under subsection (1) must require a member of a law enforcement agency or an investigator who is accompanied by a member of a law enforcement agency to access or seize the article in question and, to that end, authorizes the member of a law enforcement agency or an investigator who is accompanied by a member of the law enforcement agency to—

(e) access and search any data, a computer device, a computer network, a database, a critical database, an electronic communications network or a National Critical Information Infrastructure identified in the warrant to the extent as is set out in the warrant;”

The ICT ECSPs submit that the provision empowers the State to seize control of information held by the ECSPs under the guise that this is related to cybercrime - there is the possibility that such information will not relate to cybercrime. Furthermore, the Bill does not adequately deal with issues regarding privacy and protection of personal information. Accordingly, the ICT ECSPs request clarity on the search and seizure powers granted to the State and how these provisions will not be in conflict with the relevant privacy laws/personal information laws and constitutional rights of customers of the ICT ECSPs.

Furthermore, the current wording suggests that the State may seize the actual electronic communications network of the ICT ECSPs, which is unnecessary and not practical. It is therefore concerning that such extensive seizure powers have been granted to the State through the Bill. The ICT ECSPs therefore submit that limitations need to be specified in the warrant and such limits should only be confined to access control (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 posed to the network of the Electronic Communications Service Provider will be identified and addressed in the access control layer of the network.

It is further submitted that no clarity has been provided in the Bill in respect of the powers that are to be granted to the “investigator” as contained in Section 29(2)(e) of the Bill. If the search and seizure warrant is to be effected by a member of law enforcement agency, it would be superfluous for an investigator to accompany such member of a law enforcement agency to affect the search and seizure. This is especially so given the fact that the roles and responsibilities of the investigator have not clearly been defined. To this end ICT ECSPs request that the Bill define the powers, roles and responsibilities of an investigator referred to in chapter 4 of the Bill.

Moreover, Section 29(1)(ii) of the Bill states as follows : “being used or is involved in the commission of an offence”. It is submitted that the provision of this section in the Bill needs to clearly make reference that the search and seizure relates to the commission of offences in relation to cybercrime. This submission is predicated by the fact that as it stands, this particular section in the Bill can be open to abuse as there is no qualification in terms of the limitations of the search and seizure.

The DoJ should also note that the Criminal Procedure Act adequately deals with search and seizure and that there is no need for a duplication of the provisions relating to search and seizure to be incorporated into this Bill. The ICT ECSPs submit that the current procedures for search and seizure as set out in the Criminal Procedure Act are sufficient and should apply to cybercrimes. There must always be a nexus between what is being investigated and what should form the basis of items seized in an operation. The courts have extensively dealt with this aspect and have given favour to a narrower interpretation of what can and can’t be taken during a search and seizure operation.

3.4 Assisting member of law enforcement agency or investigator, Section 33(1)(b)(iv)

The proposed section seeks to impose an obligation on an Electronic Communications Service Provider, in control of inter alia computer device, computer network, electronic communications network or a national critical information structure (the items) that is subject to search warrant, to assist the law enforcement **to remove any of the aforesaid items.** The ICT ECSPs are prepared where possible to assist the law enforcement officers in the eradication, detection and/or prevention of cyber crimes. However, it is submitted that the intended measures such as the removal of any of the aforesaid items may cause severe financial loss to the ICT ECSPs. It may not even be practically feasible to remove and/or isolate any of the aforesaid items without causing severe interruptions with business operations. Further, the ICT ECSPs are obliged to comply with certain legislative requirements such as downtime, quality of service, etc. As such, removing any of the aforesaid items may lead to service providers not being able to comply with some of the legislative requirements. In addition, the ICT ECSPs have signed very strict service level agreements with their customers with the result that any removal of any of the items or any disruptions arising from the enforcement of the proposed measures may result in such service providers facing civil damages claims. The ICT ECSPs also face a possibility of losing customers. Any disruptions of this nature should therefore be avoided at all costs. Alternatively, this has to be carried out in such a manner that would result in minimal service disruptions.

The ICT ECSPs would like to re-iterate that the Criminal Procedure Act adequately deals with this aspect and therefore there no need for a duplication of the provisions relating to assisting a member of a law enforcement agency or investigator.

3.5 Obstructing or hindering member of law enforcement agency or investigator who is accompanied by member of law enforcement agency and authority to overcome resistance, Section 34

In this section, which also makes reference to the “investigator”, the ICT ECSPs iterates our concerns regarding no proper definition, which specifies the powers, roles and responsibilities of the investigator, especially where such a function can easily be performed by a member of a law enforcement agency.

3.6 Expedited Preservation of Data, Section 39

It is the view of the ICT ECSPs that the data, which needs to be preserved; relates to the offences mentioned in chapter 2 of the Bill; and would fall within the ambit of the RICA Act. The data can be divided into two groups which is defined in the RICA Act. These groups are:

1. Indirect Communication; and
2. Communication-related information

The ICT ECSPs submit that it is not in a position to preserve the data that is defined in the RICA Act as “indirect communication”. Indirect Communication is essentially electronic communications that refers to the substance, purport or meaning of that communication (i.e. the content information). The RICA Act defines Indirect Communication as: “the transfer of information, including a message or any part of a message. Whether-

(a) in the form of-

(i) speech, music or other sounds:

(ii) data:

(iii) text;

(iv) Visual images, whether animated or not;

(v) signals; or

(vi) radio frequency spectrum: or

(b) in any other form or in any combination of forms.

that is transmitted in whole or in part by means of a postal service or a telecommunication system;” Such information can only be preserved by the Office of Interception Centres when an interception direction has been served. As a result, The ICT ECSPs submits that this section in the Bill should exclude such information from being preserved by an Electronic Communication Service Provider since this information will be routed to the Office of Interception Centres and they would be in a position to preserve the content information.

We would further like to remind the DoJ that if ICT ECSPs are required to preserve the indirect communication information, this can only be done through interception of communications and as such would be in violation of section 2 of the RICA Act, which provides *that “no person may intentionally intercept to attempt or intercept, or authorize or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission”.*

The only data that ICT ECSPs preserve in respect of electronic communications is the communication-related information as defined in the RICA Act, which means: *“any information relating to an indirect communication which is available in the records of a telecommunications service provider, and includes switching, dialling or signalling information that identities the origin, destination, termination, duration, and equipment used in respect of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system” .*

The Directive in respect of different categories of Telecommunications Service Providers issued in terms of Section 30(7)(a) of RICA Act (GG: 28271 of 28 November 2005) prescribes that such information should be retained for 30 days and for up to 3 years. If such information is required all that is needed is for a law enforcement agency to submit a request to the electronic communications service provider as prescribed in the RICA Act.

Depending on whether there is any other information relating to electronic communications that would relate to an offense in terms of chapter 2 of the Bill, the ICT ECSPs submits that it is not necessary to place an obligation on Electronic Communications Service Providers in section 39 of the Bill and the reference to Electronic Communications Service Providers should be deleted.

We further submit that the application for a preservation of data order be submitted to the Designated Judge as defined in the RICA Act[[3]](#footnote-3) as opposed to the magistrate that is referred to in section 39(7) of the Bill. This is by virtue of the fact the Designated Judge would be able to more adequately apply his / her mind to the facts of the matter before granting the order for preservation of data. Additionally, and purely because the preservation order would entail an effective violation of the stipulations of RICA Act on the part of the electronic communications service provider, the Designated Judge would be able to assess whether such a violation is necessary and warranted. We note further that section 39(7) of the Bill makes reference to the presiding magistrate, whilst section 40(4)(a) of the Bill makes reference to the Designated Judge.

We submit that this will create confusion to the law enforcement agencies as well as to the Electronic Communications Service Providers in terms of the proper judicial authority responsible for preservation orders and disclosure of data directions. We reinforce our statement that a singular entity, in this case the Designated Judge, be assigned the task of issuing preservation orders and disclosure orders respectively

The Bill, in so far as it relates to section 39 fails, to adequately assess the cost implications to the Electronic Communications Service Providers in preserving data in accordance with a Preservation Order. The ability to preserve data will invariably result in the incurring of additional costs due to the fact that systems would need to be modified, additional resources employed and other ancillary costs associated with this additional requirement. There is no indication in the Bill as to where such costs are to be recovered from and whether the relevant Minister has made, or will make provisions for the Electronic Communications Service Providers to be reimbursed.

3.7 Private Sector Security Incident Response, Section 55

The ICT ECSPs submits that there are too many structures dealing with cybercrimes and cyber security matters in the Bill. Accordingly, this section should be reconsidered.

The ICT ECSPs submits that the response team should be termed “Industry Sector Security Incident Response Team” as private sector is too broad. By establishing an industry sector team, resources can be shared between ECSPs.

3.8 National Critical Information Infrastructure Protection, Section 56

3.8.1 Section 56(2) provides that the Cabinet Minister responsible for State Security will declare any information, infrastructure or information structures as national critical information infrastructure. This means that once identified the infrastructure will be declared as critical without following due process. The ICT ECSPs submit that section 56(2) should be amended to ensure that the declaration of infrastructure is fair and that all affected parties are given an opportunity to be heard. Accordingly, the ICT ECSPs proposed that section 56(2) should be amended as follows: “The Cabinet Member responsible for State Security may, subject to subsection (3), after considering any recommendations made to him or her in terms of subsection (1) or at any time, by notice in the Gazette and after consultation with the affected party, declare any information, structure, or category or class of information structures or any part thereof, as National Critical Information Infrastructure ...”

Furthermore, the regulations referenced in section 56(5) should only be made in consultation with the owners of National Critical Information Infrastructure, which will include the Electronic Communications Service Providers as defined in the Bill. Moreover, such regulations should also be industry specific and must be drafted to permit an organisation to implement acceptable industry standards.

Section 56 of the Bill makes provision for the identification and declaration of national infrastructure as critical. What is lacking however is an indication of steps that should be taken when critical infrastructure ceases to be critical or where an operator goes out of business. The ICT ECSPs submit that the Bill should clearly set out steps that should be taken where an operator or infrastructure ceases to be critical or goes out of business.

3.9 National Critical Information Infrastructure Protection, Section 58

Section 58(1) states” The Director-General: State Security must, at least once a year, cause audits to be performed on National Critical Information Infrastructures to evaluate compliance with section 56(6) of the Act...”

The ICT ECSPs submits that it is not clear from the current wording who would be entitled to audit the national critical information infrastructure or who would bear the costs of such audits. The ICT ECSPs submit that they are required to conduct regular and on-going audits on their infrastructure as part of good business practice. Accordingly, the ICT ECSPs recommend that section 58(1) should be amended to permit ECSPs to continue conducting their own audits on national critical information infrastructures and to make such audit findings available on request. Alternatively, section 58(1) should be amended to limit the required audits to access control audits.

3.10 Admissibility of affidavits, section 59

Section 59(3) of the Bill provides that “the court before which an affidavit is produced as prima facie proof of the relevant contents thereof, in its direction, cause the person who made the affidavit to be subpoenaed to give oral evidence in the proceedings in question ...”

The general rule in both criminal and civil proceedings is that evidence should be given viva voce, i.e orally in an open court by sworn witness. The principle of viva voce evidence however does not necessarily mean that the witness should be physically present in an open court. The rule could also be satisfied by sign language or where the witness writes down his or her answers. Due to the time consuming nature of viva voce evidence our courts have relaxed the rules and have instead replaced this with the admission of affidavits to replace oral evidence especially for non-contentious matters or where the issues are such that the behaviour or character of the witness is not considered essential. The Criminal Procedure Act contains a number of provisions permitting evidence to be given on affidavit (which provides prima facie proof of the matter in question).

To this end ICT ECSPs submit that witnesses should be subpoenaed to give oral evidence in a court of law as a last resort (not as a matter of the discretion of the presiding officer) and where there is a genuine dispute of fact that cannot be resolved without hearing witnesses.

3.11 General Obligations of ECSPs, Section 62 and Section 63

Section 62 of the Bill refers to the further obligations on Electronic Communications Service Providers, who must take all reasonable steps to prevent the use of its computer network or electronic communications network for the commission of an offence provided for the Bill. Section 63 of the Bill prescribes the liability provisions that apply to Electronic Communications Service Providers who fail to take these reasonable steps.

The ICT ECSPs submits that clarity the DoJ clarify on the reasonable steps that must be taken by Electronic Communications Service Providers (section 62(1). Alternatively, the ICT ECSPs propose that these reasonable steps should be replaced with the requirement to co-operate with the relevant Law Enforcement Agency who would be involved in identifying and addressing cybercrimes and or cyber security threats. As such section 62 should therefore be amended as follows:

Section 62 should read as follows:

“62(1) An electronic communications service provider, **shall, once it has been established that its computer network or electronic communications network has been utilised for the commission of an offence as provided in this Act, undertake to provide its full cooperation with the relevant Law Enforcement Agency tasked with investigating the specific cybercrime that has been committed.**

62(2)An electronic communications service provider that **has become** aware that its computer network or electronic communications network **has been utilised for the commission an offence in terms of this Act; shall after having reported the matter to the relevant law enforcement agency, or after having been informed by the relevant law enforcement agency;**

(a) **Take such measures as it deems fit, in accordance with its own information system policies, processes and procedures, to mitigate the impact of the offence;**

(b) **Assist and co-operate with the relevant law enforcement agency in terms of furnishing such information as may be required by the law enforcement agency for the investigation of the offence, where such assistance and cooperation is in accordance with the laws of the country relating to disclosure of information that is held by the electronic communications service provider.”**

In respect of section 63, it follows that an Electronic Communications Service Provider who is not seen to be co-operating in the identification and mitigation of cybercrimes and or cyber security related risks will therefore be exposed to liability provisions.

4. Conclusion

In light of the above, the ICT ECSPs would like to reiterate the following:

4.1. Structures dealing with Cybercrime

* The precise nature of the support that is to be rendered by the relevant structures and the roles and responsibilities for each structure needs to be clearly defined; and
* The Bill should clarify the relationship between various structures dealing with cybercrime

4.2. Defining Cybercrime

* The Bill should define the concept of cybercrime taking into account its characters and that it differs in material respect from the traditional forms of crime.

4.3. National Critical Information Infrastructure Protection

* The declaration of infrastructure should be fair and ensure that all affected parties are given an opportunity to be heard; and
* The Bill should clearly set out steps that should be taken where an operator or infrastructure ceases to be critical or goes out of business.

4.4. General Obligations of Electronic Communications Service Providers

* The DoJ should provide clarity on the reasonable steps that need to be taken by Electronic Communications Service Providers to prevent the unlawful use of its network;
* Alternatively, the reasonable steps should be replaced by the requirement to co-operate with the relevant Law Enforcement Agency; and
* It should be noted that the ICT ECSPs have existing mechanism to block child pornography when brought to our attention.

The ICT ECSPs trusts that the DoJ will consider the merits of our submission before the Bill is sent to Cabinet and to keep in mind the financial, administrative and business risk burdens imposed on our business and the impact to our customers.

**END**

1. PoPI defines personal information as: information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

   (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

   (b) information relating to the education or the medical, financial, criminal or employment history of the person;

   (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

   (d) the biometric information of the person;

   (e) the personal opinions, views or preferences of the person;

   (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

   (g) the views or opinions of another individual about the person; and

   (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person; [↑](#footnote-ref-1)
2. 2PoPI defines Data Subject as “a person to whom personal information relates”. [↑](#footnote-ref-2)
3. The RICA Act defines a Designated Judge as any judge of a High Court discharged from active service under section 3(2) of the Judges’ Remuneration and Conditions of Employment Act, 2001 (Act 47 of 2001), or any retired judge, who is designated by the minister to perform the functions of a designated judge for purposes of this Act. [↑](#footnote-ref-3)