The Chair person of the Justice Portfolio Committee

Parliament

25 July 2017

RE: Written submissions to parliament regarding the Cybercrimes and Cybersecurity Bill-2017

Dear Sirs

Introduction

The purpose of this commentary is to discuss the application and effectiveness of the recently published Cybercrimes and Cybersecurity and Related Matters Bill[[1]](#footnote-2) in relation to the applicable sections which have been discussed in this commentary. Further the this commentary explores whether or not the Bill addresses the shortcomings which have been identified in the ECT Act.

Most cybercrime acts are estimated to originate in some form of organised activity, with cybercrime black markets established on a cycle of malware creation, computer infection and botnet management.[[2]](#footnote-3) This includes the harvesting of personal and financial data, data sale and selling of financial information which are reasonable simple to carry out. Cybercrime perpetrators no longer require complex skills or techniques.[[3]](#footnote-4) Globally, cybercrime shows a broad distribution across financially driven acts and those relating to computer, as well as acts against the confidentiality, integrity and accessibility of computer systems. However, globally police recorded crimes statistics do not represent a sound basis for determining the precise impact of cybercrimes.[[4]](#footnote-5)

According to Cassim cybercrime differ from other crime in that it operates within a highly organised system making it more likely to create beneficial effects that outweigh its costs, and the perpetrators usually possess a particular psychology that make them almost immune to more innovative law enforcement method.[[5]](#footnote-6) For example the use of the internet to facilitate and commit acts of terrorism is a real occurrence that often can only be dealt with after the event, with the perpetrators even literally getting away with murder.

Cyber-attacks are typically intended to disrupt the proper functioning of the target, such as computer systems, servers or underlying infrastructure, especially if these systems are part of critical information infrastructures of a country, among others, by means of unlawful access, computer virus or malware.[[6]](#footnote-7) With the above having been said, it will be imperative to examine the scope and application of the Bill.

Application of the Bill

The preamble of the Bill on Cybercrime states that its purpose is among other things:

*To create offences and impose penalties to further regulate their powers to investigate, search and access or seize; to further regulate aspects of international cooperation in respect of the investigation of cybercrime; to regulate jurisdiction; establishment of various structures to deal with cybersecurity; to regulate National Critical Information; to regulate aspects relating to evidence and to impose obligations on electronic communication service providers regarding aspects which may impact on cybersecurity.*

For purposes of this commentary only the application of sections 2, 3, and 5 including sections 12 of the Bill on Cybercrime are discussed. These sections make provision for offences regarding personal and financial information or data related offences, unlawful access and unlawful interception of data that are the provision which have been discussed and have been discussed in Chapter 2 of this dissertation.

Section 3 of the Bill regulates unlawful acquiring if data offences of any person who unlawfully and intentionally acquires by any means or possesses or uses or provides this information to another person to another person. The use of personal or financial information of another person for purposes of committing an offence is punishable under the Bill and the offender will be found guilty of such an offence.[[7]](#footnote-8) In addition, any person who is found in possession of personal or financial information of another person to which there is a reasonable suspicion that such information was acquired, is possessed or is to be provided to another person for purposes of committing an offence and is unable to give satisfactory exculpatory account to such possession is guilty of an offence.

The discussion pertaining to this provision is based on the fact that information or data can be the subject of several constitutive acts, namely; the act of obtaining, possessing and using identity related or financial information or data. Personal or financial information or data can be for example, obtained via illegal access to a computer device and database, the use of phishing or interception tools or through illicit acquisition. Examples of this are acts such as dumpster diving,[[8]](#footnote-9) social engineering,[[9]](#footnote-10) theft and online buying of information or data of another person.[[10]](#footnote-11)

Further, financial information or data is a popular target in cyberspace. Financial information or data which is targeted in cyberspace is information pertaining to savings accounts, credit cards, debit cards and financial planning information.[[11]](#footnote-12) Personal or financial information or data are mostly used to commit financial cybercrimes. The above mentioned offences provided for in this particular section, aim to address personal or financial information or data related offences.[[12]](#footnote-13)

Section 2 of the Bill regulates unlawful access and criminalises the unlawful accessing of the whole or any part of data, a computer device, a computer network, a database, a critical database, an electronic communications network or national critical information infrastructure.[[13]](#footnote-14)With regards to this section, illegal access is not the end goal to an offence but rather the first step towards further crimes such as interfering with or intercepting data. Since the development of computer networks, its ability to connect has been used by hackers for criminal purposes.[[14]](#footnote-15) Hackers need not be present at the crimes scene; they just need to circumvent the protection securing the database, network or computer device.[[15]](#footnote-16)

The criminalisation of illegal access represents an important deterrent for many other subsequent acts against the confidentiality, integrity and availability of data and related devices.[[16]](#footnote-17) Thus, to address the above mentioned this section criminalises the unlawful accessing of the whole or any part of data or any related device.[[17]](#footnote-18) A legal interest is infringed, not only when a person unlawfully interferes or commits other unlawful acts in respect of data, a computer device, a computer network or database or an electronic communications network, but also when a perpetrator for example, merely accesses a computer network. Illegal access does not require the offender to access system files or other stored data.[[18]](#footnote-19)

Lastly Section 5 of the Bill regulates unlawful interference of data and provides that any person who unlawfully and intentionally intercepts data to, from or in a computer device, a computer network, a database, a critical database, an electronic communications network or a national critical information infrastructure or any part thereof is guilty of an offence. The criminalisation of this act aims to protect the integrity, privacy and confidentiality of data within a computer device, a computer network, a database or an electronic communications network. Unlawful access allows the perpetrator to carry out further actions to acquire data unlawfully. Thus, the use of information communication technologies is accompanied by several risks related to the security of information transfer.

In addition to illegal access, Section 12 of the Bill provides that any person who attempts, conspires with another person; or aids, abets, induces, incites, instigates, instructs, commands or procures another person to commit an offence is in terms of this chapter, guilty of an offence and is liable on conviction to the punishment applicable to someone convicted of actually committing that offence.

Various online communities exist in order to facilitate cybercrimes and are sometimes in accordance with their ideological principles.[[19]](#footnote-20) An example of co-operation in cybercrime is where a person obtains information through social media and gives it to a hacker to gain access to a server, on which certain information is copied, it in turn is given it to another person who sells the information or uses the information to commit fraud or computer related extortion. The application of the Bill particularly, provisions which deal with addressing cybercrimes in South Africa, has attempted to address the shortcomings identified in ECT Act.

How the Bill has addressed ECT Act identified shortcomings

As mentioned earlier this dissertation focuses on sections 2, 3, 5 and 12 of the Bill in comparison to Chapter 13 of the ECT Act and in particular sections 86 to 89.

Firstly Chapter 2 of this paper, briefly looked at the shortcomings of the ECT Act with the following aspects being identified; that the penalties under sections 86 to 89 of the ECT Act are not harsh enough and lastly that there have been promises of cyber inspectors but no

 The Bill, however, imposes harsh penalties, for an offence that is committed and when the perpetrator is found guilty of the said offence. The penalties range from a fine with a minimum amount of 5 million rand to a maximum of 10 million rand. The period for imprisonment provided for is a minimum of 5 years to a maximum of 10 years. The Bill also makes provision for the imposition of both a fine and imprisonment on conviction.[[20]](#footnote-21) This can be noted as a substantial improvement moving forward from the ECT Act and that the Bill has definitely provided for harsher fines and longer periods of imprisonment.

Commentary on the Bill

Various academics have had different opinions regarding the Bill and the impact the Bill has on the law in South Africa and whether such an establishment will be to the benefit or detriment of the country.

Duncan is of the opinion that the draft law’s promise to make the internet a much safer, freer space for South Africans is illusory.[[21]](#footnote-22)Duncan writes that the Bill threatens digital rights in significant ways, especially the freedom of expression and association, and the right to privacy. It is also observed that the Bill lacks important checks and balances, and increases

Duncan adds that the Bill creates a host of new state institutions which fall under several state departments, to counter cybercrimes and cyber terrorism. Hence, Duncan states that the Bill will hand indirect control of the internet to South African spies. Further to this, Duncan says that state security is not the most appropriate institution to be tasked with this responsibility as it leans towards secrecy and its existing activities which lack democratic controls.[[22]](#footnote-23)

He goes further and says that the Bill resists the temptation to over criminalise online behaviours such as spamming and that this remains a ground for concern. In addition, it is noted that the Bill amends RICA by adding additional offences. Duncan states that its drafters argue that the Bill and the Criminal Procedure Act[[23]](#footnote-24)do not contain adequate measures to investigate cybercrimes.

Duncan writes that it does have important public purposes, for instance, that it criminalises acts such as unlawful interception of and interference with data, as well as computer related fraud and cyber terrorism, and regulates foreign co-operation to fight these cries. It protects critical information and infrastructure by making it illegal to interfere with them.[[24]](#footnote-25) He concludes by saying that on a broader level, governments including the South African government need to acknowledge that they have helped to create the enormous problem which they are legislating against. They have vested interest in promoting communications networks that are built for vulnerability rather than for resilience, because they want to maintain their ability to spy on their citizens.[[25]](#footnote-26)Commentary from the Right2Know Campaign[[26]](#footnote-27) notes that this Bill forms part of a set of laws and policy initiatives in South Africa that aims to regulate the ever expanding online economy, as well as the surge in cyber related crimes (locally and internationally).[[27]](#footnote-28) The Campaign also states that the current legal framework to combat cybercrime is a hybrid of legislation and the common law. The common law however, takes its approach on a case by case basis, thus has not kept pace with the dynamic nature of cybercrimes. The Right2Know Campaign is of the opinion that the Bill is a product of calls by various stakeholders for government to enact specialised legislation and to align South Africa with international practice.[[28]](#footnote-29)

Furthermore, that if passed the legislation will codify numerous offences or ‘cybercrimes and their related penalties. What is more, the Right2Know Campaign says in essence, the Bill criminalises unlawful access to and interception of data; provides local authorities with extensive powers of investigation, search, access and or seizure; imposes various obligations on electronic communications service providers and regulates jurisdiction of the courts, specifically in relation to cross border offences.[[29]](#footnote-30) However, the Right2Know Campaign criticises the Bill in that they state that the seven deadly sins of the Bill are that it:[[30]](#footnote-31)

(1) Hands over control of the internet to the Minister of State Security,
(2) Gives the state security structures the powers to effectively declare ‘national key points’ of the internet- and potentially grants backdoor access to any network,
(3) Criminalises journalists and whistle-blowers by sneaking in the worst parts of the disputed ‘Secrecy Bill’,
(4) Increases the state’s surveillance powers and is even more invasive than RICA,
(5) Undermines South African’s civil liberties and particularly the constitutional rights to privacy,
(6) Contains 59 new criminal offences involving computer usage – many of which are so broad that they could ensnare ordinary computer users, and
(7) Contains anti- copyright provisions so harsh you could be charged for even posting a meme.

The Bill also considers suspects guilty until proven innocent. The Right2Know Campaign suggests that the solution would be to scrap the entire Bill and start from scratch with proper public participation and protection as well as aiming to preserving the democratic spirit of the right to privacy.[[31]](#footnote-32)

Similarly, Tshongweni[[32]](#footnote-33) is of the opinion that currently South Africa has no legislation that addresses cybercrimes, whether it describes what constitutes a cybercrime, how to enforce the law governing cybercrime or to determine appropriate correctional sentencing for those convicted of offences within this realm.[[33]](#footnote-34)

Tshongweni states that the Bill is timeous in that it proposes legislation that will bring South Africa in line with international laws governing internet based crimes. However, Tshongweni is of the view that the Bill is excessively far reaching, beyond practical plausibility in many instances and that it grants a concerning level of discretion to the State’s Security Cluster.[[34]](#footnote-35)

The Law Society of South Africa[[35]](#footnote-36) has also made their submissions[[36]](#footnote-37)on the Bill. In this dissertation only a few of their submissions will be noted. LSSA submits that the Bill goes in the right direction in extending the list of substantive cybercrimes which were initially limited in the ECT Act like unauthorised access to, interception of, or interference with data.[[37]](#footnote-38) LSSA submits that the Bill accordingly expands that types of offences originally covered under the ECT Act and also criminalises more activities relating to the unlawful use of computer systems.[[38]](#footnote-39)

LSSA further submits that it is of great concern that the Bill will be amending more than 16 already existing laws, and that there will inevitably be unintended consequences which have to be minimised as far as possible with a longer period of consultation.[[39]](#footnote-40) Furthermore, a Bill of this magnitude should not be rushed through Parliament and it should be able to withstand constitutional scrutiny on aspects of privacy, the right to dignity and freedom of expression. LSSA believes that in the Bill’s current state, it will not pass constitutional scrutiny and it ought to be substantially revised.[[40]](#footnote-41)LSSA further states that the Bill does not cover all principles as contained in the COE. LSSA raises concern about the extent to which attention has been provided to harmonise the legislation with that of other countries. Lastly, LSSA submits that greater consultation and research needs to be undertaken by the Justice and Constitutional Department.[[41]](#footnote-42)

Conclusion

Firstly that the specific conduct criminalised and any study of cybercrime offences must take into account the Criminal Procedure Act as this is law that deals with issues applicable to all offences. Secondly, when analysing the functions of cybercrime legislation, there are several aspects which needs to be taken into account, namely; setting clear standards of behaviour for the use of computer devices; deterring perpetrators and protecting citizens; enabling law enforcement investigations while protecting individual privacy; providing fair and effective criminal justice procedures; requiring minimum protection standards in areas such as data handling and retention and enabling co-operation between countries in criminal matters involving cybercrime and electronic evidence. When looking at the above mentioned aspects we have to compare this to the Bill and analyse whether the Bill has met these standards and if so, to what extent.

The last aspect, is comparing whether the Bill has in actual fact addressed the shortcomings identified in the ECT Act. From the preceding discussion, there is a clear indication that the Bill has addressed to a great degree of the shortcomings in that the Bill does provide for harsher penalties than those imposed in the ECT Act.

With regard to the cyber inspectors in the ECT Act which were created but never implemented, the Bill has addressed this issue to the extent that it has created a Cybersecurity Structure under the control of the Director General of State security who will control the regulation regarding cybercrime and cyber terrorism. To this extent the Bill has addressed the shortcomings of the ECT Act. However, with regards to the shortcoming relating to the extent of the state control in relation to the regulation of cybercrimes, the Bill has not addressed these. With reference to the opinions mentioned previously in this chapter, we submit that the state is given extensive control over the regulation of cybercrimes and the contents thereof. In particular the state is provided with too much control over how businesses and private persons communicate over the internet. One can therefore conclude that the Bill has addressed majority of the shortcomings which have been identified in the ECT Act and that, although it has deal with such issues, the Bill has its own shortcomings.

Notwithstanding the above written submissions which have been made, we wish to further make oral representations to the justice portfolio committee.

Regards

Sizwe Lindelo Snail Ka Mtuze Attorney at Snail Attorneys

Charlotte Schultz Attorney at Legal-Aid South Africa

1. Published in Government Gazette, volume 603, 2 September 2015, number 39161, herein after referred to as ‘the Bill’. [↑](#footnote-ref-2)
2. Consultation document on Cyber Crimes and Cybersecurity Bill, www.justice.gov.za (accessed 20 October 2015) 1. [↑](#footnote-ref-3)
3. Consultation document (2015) 2. [↑](#footnote-ref-4)
4. *Ibid.*  [↑](#footnote-ref-5)
5. Cassim (2009) 40. [↑](#footnote-ref-6)
6. Cassim (2012) 385. [↑](#footnote-ref-7)
7. The Bill on cybercrime, section 3. [↑](#footnote-ref-8)
8. Dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. [↑](#footnote-ref-9)
9. Social engineering is an attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures [↑](#footnote-ref-10)
10. An example of social engineering is phishing and spear phishing [↑](#footnote-ref-11)
11. Consultation Document (2015) 4. [↑](#footnote-ref-12)
12. *Ibid.* [↑](#footnote-ref-13)
13. The Bill on cybercrime section 4. [↑](#footnote-ref-14)
14. Consultation Document (2015) 5-6. [↑](#footnote-ref-15)
15. *Ibid.* [↑](#footnote-ref-16)
16. *Ibid.* [↑](#footnote-ref-17)
17. *Ibid.* [↑](#footnote-ref-18)
18. *Ibid.* [↑](#footnote-ref-19)
19. Consultation Document (2015) 30. [↑](#footnote-ref-20)
20. Development has occurred in that regard. When looking at the penalties which the ECT Act has imposed, these ranging from a fine or imprisonment not exceeding twelve months, are not considered as harsh penalties and that harsher penalties should be imposed. [↑](#footnote-ref-21)
21. Duncan ‘A new Bill threatens our digital rights and raises the spectre of internet censorship.’ www.mailandguardian.co.za. [↑](#footnote-ref-22)
22. *Ibid.* [↑](#footnote-ref-23)
23. Act 51 of 1977. [↑](#footnote-ref-24)
24. Duncan, 2. [↑](#footnote-ref-25)
25. Duncan, 6. [↑](#footnote-ref-26)
26. Right2Know campaign: ‘Legislation: concerns over proposed cyber law’, October 2015 www.Right2knoww.org.za (accessed 20 October 2015). [↑](#footnote-ref-27)
27. *Ibid.* [↑](#footnote-ref-28)
28. *Ibid.* [↑](#footnote-ref-29)
29. Bernstan, Ebrahim, Obane ‘Concerns raised over SA cybersecurity law’ www.news24.com (accessed 20 October 2015) [↑](#footnote-ref-30)
30. Right2Know campaign: ‘What’s wrong with the Cyber Crimes Bill-The seven deadly sins’, www.right2know.org.za (accessed 30 November 2015). [↑](#footnote-ref-31)
31. *Ibid.* [↑](#footnote-ref-32)
32. M. Tshongweni, Concerns raised over Cybercrime and Cybersecurity Bill in SA, www.itnewsafrica.com (accessed 22 September 2015). [↑](#footnote-ref-33)
33. *Ibid.* [↑](#footnote-ref-34)
34. *Ibid.* [↑](#footnote-ref-35)
35. Herein after referred to as ‘LSSA’. [↑](#footnote-ref-36)
36. Comments by the Law Society of South Africa on the Cybercrimes and Cybersecurity Bill’, www.lssa.org.za (accessed 30 April 2016). [↑](#footnote-ref-37)
37. *Ibid.* [↑](#footnote-ref-38)
38. *Ibid.* [↑](#footnote-ref-39)
39. *Ibid.* [↑](#footnote-ref-40)
40. *Ibid.* [↑](#footnote-ref-41)
41. *Ibid.* [↑](#footnote-ref-42)