A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa

TERRINA FRANCINE GOVENDER

Student Number: 208504899

This Research Project is submitted in partial fulfilment of the regulations for the LLM Degree at the University of KwaZulu-Natal

College of Law and Management Studies
School of Law

Supervisor: MR LEE SWALES

DECLARATION

I declare that this project is an original piece of work, unless specifically indicated to the contrary in the text, which is made available for photocopying and inter-library loan.

TF Govender

TERRINA FRANCINE GOVENDER

JANUARY 2018

ACKNOWLEDGEMENTS

I wish to express my heartfelt and sincere gratitude to the following people:

- My supervisor, Mr. Lee Swales, for his continued guidance, words of wisdom and administrative assistance in ensuring the successful completion of this dissertation.
- My husband, Keagan Govender for his love, support and endless encouragement to persevere throughout the journey of this dissertation.
- My parents, family and friends, for all their prayers, motivation and continued support.
- My Lord and Saviour, Jesus Christ, through Him all things are possible.

Table of Contents

CHAPTER ONE - INTRODUCTION

1. Background

1.1. The evolution of cybercrime

As the internet continues to evolve and people become more reliant on it, individuals, communities and nations are becoming increasingly vulnerable to the threat of the cyber-criminal.[1] Due to intensified media attention[2] and a number of recent sophisticated cyber-attacks,[3] the impression has started to form that cyber-incidents are becoming more frequent, more organised, more costly and altogether more dangerous.[4]

In South Africa, the Department of Justice estimated that the damage caused by cyber-related offences is around one billion Rand annually.[5] More specifically, the Norton Report[6] revealed that the third highest number of cybercrime victims globally belong to South Africa experiencing a loss in excess of R2.2bn due to internet fraud and phishing attacks annually.

[1]P Hunton 'A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment' (2011) 7 *Digital Investigation* 1.

[2]There is an increasing amount of focus on cybercrime in the media recently. For instance, the FBI made public their most wanted list for cybercrime (M Park 'Meet the FBI's top 5 Most Wanted for cyber crimes' CNN and cyber attacks on the TalkTalk website and NASA were highlighted ('TalkTalk hack attack: Friends admit cyber crime charges' BBC News.

[3]South Africa is believed to be affected by the biggest global cyberattack. This attack occurred through hackers who gained access to more than 100,000 computers globally and used malware to hold these computer systems hostage until money was paid to unlock it. Sixteen hospitals in the United Kingdom were shut down due to patient files becoming inaccessible by hospital staff. T Mulaudzi 'SA affected in Global Cyberattack' *Eyewitness News* 13 May 2017.

[4]MD Cavelty 'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities' 2014 *Science and Engineering Ethics* 702.

[5]'The Department of Justice and Constitutional Development Justice publishes Cybercrimes and Cybersecurity Bill for public comment' 28 August 2015.

[6]This report is based on research that is conducted to analyse the current state of cybercrime and the impact it has on consumers. '2013 Norton Report' *Business Media Mags*.

Cyberspace and the internet[7] have become essentials in the world today.[8] In 2016 the estimated number of internet users in South Africa was recorded at 28 580 290 which is roughly 52 percent of the South African population.[9] The fast development of technology is a huge advantage benefiting society in fields such as medicine, information technology and communications, engineering and the sciences.[10]

However, in as much as there are many benefits that the advances in technology hold, there are also disadvantages in that it carries the potential to be exploited by criminal activities such as computer-based fraud, sexual exploitation and illegal interception of private communications.[11] Van der Merwe suggests that a computer is just another tool that criminals can use to commit crimes which now fall under the umbrella of 'information and communications technology' ('ICT') crime.[12]

There are various types of cybercrimes threatening society today, with one of its definitions being 'any criminal activity that involves a computer'.[13] This can be further divided into two categories, the first being any crime that has not been in existence before the advent of the computer and is reliant on the computer for execution; for example, hacking, cracking, sniffing and the production and dissemination of malicious code are examples of such crimes. The other category is crimes that have been in existence for centuries but have now started to be performed in the cyber environment – internet fraud, possession and distribution of child pornography, to name a few, form part of this category of cyber-crime.[14]

---

[7] Cyberspace differs from the internet in that 'Cyberspace denotes the "place" where communication on the internet takes place and exists everywhere that there are telephone wires, coaxial cables, optical fibres cables or electromagnetic waves.' S Papadopoulos et al. *Cyberlaw@SA III The law of the internet in South Africa* 3ed (2012) 335.

[8] As at 31 March 2017 there are an estimated 3, 731, 973, 423 internet users trustingly participating in sending, receiving, storing, uploading and downloading data in this sphere. 'Internet World Stats' available at http://www.internetworldstats.com/stats.htm accessed on 14 April 2017.

[9] 'South Africa Internet Users' *Internet live Stats* available at *http://www.internetlivestats.com/internet-users/south-africa/,* accessed on 14 April 2017.

[10] JB Hill and NE Marion *Introduction to Cybercrime: Computer crimes, laws, and policing in the 21st century* (2016) 10.

[11] M Grobler et al 'Preparing SA for Cyber Crime and Cyber Defense' (2013) 11(7) *Journal of Systemics, Cybernetics and Informatics* 36.

[12] DP Van der Merwe et al *Information and Communications Technology Law* 2 ed, (2016) 63.

[13] S Snail 'Cyber Crime in South Africa – Hacking, cracking, and other unlawful online activities', 2009(1) *Journal of Information, Law & Technology (JILT)* 2.

[14] *Ibid*.

Cybercrime has become a pressing reality in society. According to the Cyber Crime and Cyber Security Trends in Africa report,[15] statistics show that of the 602 million victims of cybercrime globally, 8.8 million were South Africans in the past year alone. One would expect that with the high number of cybercrime victims would come a high rate of cybercrime prosecutions and convictions. However, according to the latest SAPS crime statistics,[16] there have been no recorded convictions in this category of crimes.

This research is premised on the fact that a lack of cybercrime convictions in South Africa is directly linked to the current legislation that governs the search and seizure of electronic evidence, and its practical application being inadequate and out of date. This dissertation will aim to critically analyse the legislation that governs search and seizure of electronic evidence with a view to proposing amendments and/or solutions to address the lack of cybercrime convictions in South Africa.

It is important to note that the search and seizure of electronic evidence is not limited to cybercrime but can feature in most areas of law such as civil litigation, labour proceedings and administrative tribunals. Electronic evidence includes social media, emails, voice recordings, WhatsApp messages and the like.[17] However, to provide a more nuanced context, the analysis of search and seizure of electronic evidence in this research is limited to and discussed within the confines of cybercrime.

1.2 Search and seizure of electronic evidence in the investigation of cybercrime

The Electronic Communications and Transactions Act[18] was promulgated in 2002 and is currently the only piece of legislation that specifically regulates cybercrime in South Africa – it also governs the search and seizure of electronic evidence[19] in conjunction

[15] This report presents detailed technical data that is collected in respect of Cybersecurity trends and threats in Africa. The data is collected through voluntary country surveys which poses questions regarding the implementation of policy and legal frameworks that aim to address the technical challenges that are experienced. 'Cyber Crime and Cyber Security Trends in Africa, 2016' *Global Forum on Cyber Expertise* available at *https://www.thegfce.com/initiatives/c/cybersecurity-and-cybercrime-trends-in-africa*, accessed on 14 April 2017.
[16] Crime Statistics 2015/2016, *South African Police Service Department of Police.*
[17] E A Vincze 'Challenges in digital forensics' (2016) 17(2) *Police Practice and Research* 185.
[18] Electronic Communications and Transactions Act 25 of 2002 (hereinafter referred to as the ECT Act).
[19] S Papadopoulos et al (note 7 above; 317).

with the Criminal Procedure Act,[20] the common law, other procedural statutes,[21] and the Constitution.[22]

The ECT Act aims to, *inter alia*, promote legal certainty with respect to electronic communications and transactions, and develop a safe environment for business, consumers and government to conduct and utilise electronic transactions.[23]

The prioritisation of cyber threats in financial year 2014/2015 by the South African government, prompted the upcoming regulation of cybercrime and aspects of search and seizure by the Cybercrimes and Cybersecurity Bill.[24] The Bill aims to identify cyber-related offences and criminal liability associated with these crimes.[25] It further imposes penalties related to cybercrime and regulates the powers of investigation of cybercrime.[26]

The Department of Justice and Constitutional Development has introduced the Cybercrimes and Cybersecurity Bill in its process of reviewing and aligning current cybersecurity laws[27] to the National Cybersecurity Policy Framework. This Framework[28] provides, *inter alia*, measures to address cybercrime irregularities and to develop, review and update existing substantive and procedural laws.

With cybercrime being committed in a different environment than physical crime, the type of evidence differs too, requiring a change in legal procedures and Information and Communication Technology ("ICT") forensics.[29] In the physical world, searching

[20] Act 51 of 1977 (hereinafter referred to as the "CPA").
[21] Civil Proceedings Evidence Act 25 of 1965 and the Law of Evidence Amendment Act 45 of 1988.
[22] Constitution of the Republic of South Africa, 1996 (hereinafter referred to as the "Constitution").
[23] Section 2 of the ECT Act.
[24] Cybercrimes and Cybersecurity Bill B-2017 (hereinafter referred to as the "Bill").
[25] N Mapisa-Nqakula 'Justice, Crime Prevention and Security post-SoNA Cluster media briefing' 2015 Government Communications.
[26] Memorandum on the objects of the Cybercrimes and Cybersecurity Bill (2017) 25.
[27] Media Briefing: Statement by the Deputy Minister of justice and Constitutional Development, the Hon JH Jeffery, MP on the new proposed Cybercrime and Cybersecurity Bill, 19 January *2017 Department of Justice and Constitutional Development*.
[28] 'This South African National Cybersecurity Policy Framework is necessitated to ensure a focussed and an all-embracing safety and security response in respect of the Cybersecurity environment and establishes and addresses issues such as development and implementation of a government led cybersecurity approach to cybersecurity threats and fighting cybercrime through the promotion of coordinated approaches and planning and the creation or required staffing and infrastructure.' The National Cybersecurity Policy Framework, 2015.
[29]DP Van der Merwe … et al (note 12 above; 63).

for evidence at a crime scene would include fingerprints, DNA, gunpowder residue and the like, however the search for electronic evidence includes artefacts and electronic equipment that would indicate use, ownership or possession of electronic evidence.[30]

Therefore it is clear that the foundation of search and seizure of evidence shifts from the 'material world to the virtual world of cyberspace.'[31] As opposed to tangible evidence, digital evidence[32] can be found, for example, on electronic devices left behind at the scene of a crime[33] and in order to successfully arrest and prosecute criminals, consistent and clearly defined forensic procedures need to be followed by investigators.[34] Consequently, the field of ICT forensics[35] is aimed at utilising proven methods to preserve, collect, identify, analyse and interpret electronic evidence derived from electronic sources for the purpose of presenting this evidence before a court of law.[36]

This research will focus on the search and seizure of electronic evidence in South Africa, in the context of cybercrime. The primary legislative mechanisms that currently regulate search and seizure of electronic evidence in South Africa are the CPA[37] (provides search and seizure procedures), and the ECT Act (provides cyber inspectors with additional powers of search and seizure).[38] The Bill will be studied as it is the proposed future law that will govern the cyber or electronic environment.

---

[30] S C McQuade *Encyclopaedia of Cybercrime* (2009) 29.
[31] GP Bouwer 'Search and seizure of electronic evidence: Division of the traditional one-step process into a new two-step process in a South African context' (2014) 2 *SACJ* 156.
[32] Digital evidence and electronic evidence will be used interchangeably in this research paper.
[33] JB Hill and NE Marion (note 10 above, 105).
[34] M Reith et al… 'An Examination of Digital Forensic Models' 2002 (1) *International Journal of Digital Evidence* 2.
[35] ICT Forensics is a separate complex topic that requires far more in depth discussion which is not included in this paper however it is worth mentioning as the practical implementation of the search and seizure of electronic evidence requires the application of techniques that are foundational to ICT forensics.
[36] V Baryamureeba and F Tushabe 'The Enhanced Digital Investigation Process Model' 2004 *The Digital Forensic Research Conference* 4.
[37] Defined (note 20 above).
[38] A Irons and J Ophoff 'Aspects of digital forensics in South Africa' 2016(11) *Interdisciplinary Journal of Information, Knowledge, and Management* 277.

2. Overview of the current South African legislation relevant to the search and seizure of electronic evidence

It is critical to acknowledge that in any criminal matter in South Africa, the Constitution must be considered in the context of an accused person's right to a fair trial where evidence is unconstitutionally obtained.[39] However, the constitutional court has decided that in certain instances, even evidence that has been obtained unconstitutionally can be admitted into evidence.[40]

2.1 The Constitution

The Constitution is the sovereign law of South Africa and since its enactment, additional constraints have been imposed on the powers of search and seizure.[41] The relevance of analysing the Constitution is that if evidence is unlawfully obtained (by infringing a Constitutional right), it may well be inadmissible and render the trial unfair.[42] That being said, constitutional rights are not absolute – moreover, judicial discretion will dictate whether unconstitutionally obtained electronic evidence will be admissible or not.[43]

Search and seizures that are authorised by law (whether by statute or common law) are established as lawful but those enabling laws can be criticised for infringing on constitutional rights.[44]

[39] M Watney 'Admissibility of Electronic Evidence in Criminal Proceedings: An outline of the South African Legal Position' 2009 *JILT* 39.
[40] *Key v Attorney-General, Cape Provincial Division* 1996 (6) BCLR 788 (CC).
[41] V Basdeo 'The Constitutional validity of search and seizure powers in South African criminal procedure' 2009 (12) 4 *PER* 307.
[42] S 35(5) of the Constitution provides for the exclusionary rule. See also *Harvey v Niland* 2016 (2) SA 436 (ECG). In this case, the court held that gaining access to a person's Facebook account without their permission constitutes hacking and falls under the criminal conduct provided for by S86(1) of the ECT Act. It decided that the evidence extracted from Facebook was admissible even though it constituted a crime and infringed on the right to privacy. This was decided within the facts of the case and shows that constitutional rights are not absolute.
[43] PJ Schwikkard and SE van der Merwe *Principles of Evidence* 4ed (2016) 429. See also A Bellengere et al… *The Law of Evidence in South Africa: Basic Principles* (2013) 76.
[44] I Currie and J De Waal *The Bill Of Rights Handbook* 6ed (2013) 309.

The issue is that the right to a fair trial can be infringed by search and seizure procedures at the pre-trial stage.[45] Accused persons have the right to remain silent[46] and the privilege against self-incrimination.[47] The state bears the onus of proving its case beyond reasonable doubt, and the accused is not obliged to disclose or provide any information or documents which may strengthen or assist the state's case.[48] The discussion of the Constitution entails evaluating whether or not the accused's action of providing passwords to secure devices or removing encryption constitutes self-incrimination resulting in unconstitutionally obtained evidence.

2.2 Electronic Communications and Transactions Act 25 of 2002

The ECT Act is aimed at enabling and facilitating 'electronic communications and transactions in the public interest.'[49] The ECT Act defines electronic terms such as *data*, *IP address*, *data message* and other applicable terms; further, it criminalises specific forms of electronic conduct.[50] In addition, the ECT Act provides for the search and seizure of electric evidence.[51]

The ECT Act further makes provision for the appointment of cyber inspectors[52] and their powers; the powers to inspect, search and seize; obtaining a warrant and the preservation of confidentiality. Cyber inspectors are able to access information or enter any premises in the furtherance of an investigation into alleged cybercrime.[53] As much as this role was created and expected to become a reality,[54] there has yet to be an appointment of a cyber inspector.[55] As a result of the defunct position of the cyber inspector, the CPA and common law are relied upon in the regulation of the search and seizure of electronic evidence.

---

[45] V Basdeo 'A critique of search and seizure in terms of a search warrant in South African criminal procedure' (2015)30 *SAPL* 156.
[46] Section 35(1) (a) of the Constitution.
[47] Section 35(3) (j) of the Constitution.
[48] *Fedics Group (Pty) Ltd v Matus* 1998 (2) SA 617 (C).
[49] Section 2(1) of the ECT Act.
[50] J Omar 'Legal Terminology: Criminal Law, Criminal Procedure and Evidence' 2016 *SALJ* 229.
[51] Section 80 – Section 84 of the ECT Act.
[52] Cyber inspectors will be analysed with more detail in a future chapter.
[53] Basdeo et al (note 45 above, 153).
[54] R Weideman 'Here come the cyber inspectors' (2003) ITWeb Internet available at *http://www.itweb.co.za/index.php?option=com_content&view=article&id=81319*, accessed on 21 April 2017.
[55] *S v Miller* [2015] 4 All SA 503 (WCC) at para 56.

This dissertation will investigate whether the non-existence of cyber inspectors constitutes one of the main contributing factors to the lack of cybercrime investigations.

2.3 Criminal Procedure Act 51 of 1977

The ECT Act states that the CPA applies with the necessary changes to search and seizures in terms of this Act.[56] It is therefore an intention that these two Acts work together for the purpose of search and seizure.[57]

The CPA provides the basis of search and seizure procedures whether it is with or without a search warrant[58] and the authority to enter into premises.[59] The CPA provides for the search of any premises under certain circumstances set out in the CPA such as a search in connection with State security or any offence[60] or for the purposes of obtaining evidence.[61]

Chapter 2 of the CPA[62] governs the search and seizure of physical evidence.[63] The CPA was created in a time where data messages where not fully envisaged, and the only need was for search and seizure of tangible evidence and not electronic evidence.[64] However, the CPA can be used for collecting electronic evidence, providing 'for search warrants, searches and seizures without a warrant, the entering of premises, and the forfeiture and disposal of property connected with offences.'[65]

The issue arises from the CPA's applicability to electronic evidence with regards to cyber specific terminology and procedures. Currently the CPA is being applied to

---

[56] Section 82 (3) of the ECT Act.
[57] DP Van der Merwe (note 123 above; 87).
[58] Section 21(2) of the CPA states "A search warrant issued under subsection (1) shall require a police official to seize the article in question and shall to that end authorize such police official to search any person identified in the warrant, or to enter and search any premises identified in the warrant and to search any person found on or at such premises." See also Chapter 9 Search and Seizure of JJ Joubert…et al Criminal Procedure Handbook 11ed (2014) for more context.
[59] VG Hiemstra *Introduction to The Law of Criminal Procedure* 2ed (1985) 6.
[60] Section 25 of the CPA.
[61] Section 26 of the CPA.
[62] 51 of 1977.
[63] GP Bouwer (note 31 above; 158).
[64] E Du Toit 'Search and seizure of electronic evidence' 2016 *Commentary on the Criminal Procedure Act* 13.
[65] V Basdeo 'The legal Challenges of search and seizure of electronic evidence in South African criminal procedure: A comparative analysis' (2012) 2 South African Journal of Criminal Justice 204.

matters that include the element of electronic evidence. [66] However, there is still a need for legislation to govern the electronic environment in order to provide clarity and certainty instead of depending solely on the interpretation of the judiciary. Therefore the promulgation of the Cybercrimes and Cybersecurity Bill is expected to add to the existing legislative framework.

3. The Cybercrimes and Cybersecurity Bill[67]

This Bill was drafted with the aim of regulating cybercrimes and cybersecurity in South Africa.[68] The greater purpose of the Bill lends itself to building safer communities by enhancing cybersecurity[69] and further brings more clarity to cybercrime by creating additional offences (not defined in the ECT Act) and prescribing penalties.[70]

More specifically, with reference to the issues addressed in this dissertation, the Bill now defines previously uncertain terms such as article, computer and computer systems.[71] Chapter 5 of the Bill deals with the powers to investigate, search and access or seize, and includes the direction to the Cabinet member responsible for policing to issue Standard Operating Procedures (for the collection of electronic evidence) within six months of the enactment of the Bill.[72] These Standard Operating Procedures should be adhered to by the SAPS or any other investigating officer in the process of investigating any offence set out in the Bill.[73] This dissertation will aim to reveal how the Bill will affect the current legal position and whether it will be able to work in conjunction with the existing rules of search and seizure set out in the CPA.

---

[66] Currently electronic evidence is accepted under the definition of "document" in s 221(5) of the CPA. See *S v Harper* 1981 (1) SA 88 (D) and *S v Brown* 2016 (1) SACR 206 (WCC).This will be further discussed in the following chapter together with the need to introduce cyber specific terminology into the legislative framework.
[67] B-2017 (hereinafter referred to as "the Bill").
[68] Memorandum on the objects of the Cybercrimes and Cybersecurity Bill (2017) (note 26 above, 1).
[69] Media Briefing (note 27 above).
[70] Discussion of the Cybercrimes and Cybersecurity Bill (2015) available at *http://www.justice.gov.za/legislation/invitations/CyberCrimesDiscussionDocument2015.pdf*.
[71] Section 1 of the Bill.
[72] Section 24 of the Bill.
[73] *Ibid.*

4. International Best Practice

With constitutional principles in mind, 'when interpreting the Bill of Rights, a court, tribunal or forum must consider international law; and may consider foreign law'.[74] It is in that vein that this research paper will address international and foreign law principles regarding the search and seizure of electronic evidence.

This comparative study will be conducted with the aim of evaluating if South African legislation is line with international best practice. Stemming from this evaluation will be key lessons that South Africa can learn from other, arguably, faster developing jurisdictions in terms of legislative progressions and practical solutions of dealing with the search and seizure of electronic evidence in the cybercrime context. In this regard the Council of Europe's[75] Cybercrime Convention (hereinafter referred to as the "Cybercrime Convention"),[76] the United States of America and Australia will be studied.

The Cybercrime Convention aims to, amongst other provisions, provide for domestic criminal procedural law powers that are required for investigation and prosecution of cybercrime and the collection of electronic evidence; and making provision for administration of international co-operation.[77]

The search and seizure of electronic evidence in the United States of America must be analysed as it is known for its fast and early development of technology which unfortunately also meant that it fell victim to cybercrime much sooner.[78] As a result the legislature in the USA was quick to start creating laws to combat cybercrime.[79] Most importantly, legal rules for search and seizure of evidence are set out in Rule 41 of the

---

[74] Section 39 (1) (b) and (c) of the Constitution.
[75] 'The Council of Europe promotes human rights through international conventions, such as the Convention on Preventing and Combating Violence against Women and Domestic Violence and the Convention on Cybercrime. It monitors member states' progress in these areas and makes recommendations through independent expert monitoring bodies. For More information see https://www.coe.int/en/web/portal/home.
[76] Council of Europe Convention on Cybercrime *European Treaty Series – No. 185* available at *http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf*.
[77] Explanatory Report to the Convention on Cybercrime *European Treaty Series No. 185* available at *https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b.*
[78] DP Van der Merwe (note 12 above; 93).
[79] *Ibid.*

Federal Rules of Criminal Procedure.[80] This Rule makes provision for searching electronic storage media, seizing electronically stored information, where such media or information is concealed through technological means or where protected computers have been damaged without authorisation.[81]

The USA experiences a similar challenge as South Africa in terms of the lack of successful convictions.[82] It is important to research the manner in which the USA deals with this issue despite having electronic evidence specific legislation in place and the way in which it overcomes constitutional hurdles.

In Australia, search and seizure procedures for criminal matters are governed by the Crimes Act.[83] More importantly, this Act makes provisions for electronic searches by allowing the entrance of electronic equipment onto specified premises for the purpose of utilising forensic imaging programs in investigation.[84] Further, under this Act, the use of any electronic equipment (such as computers) that is present on the premises may be utilised.[85]

It is beneficial to compare these Acts to South African legislation in respect of defining terms and implementing specific search and seizure legislative provisions relating to electronic evidence. It is further important to review judicial decisions of the American and Australian courts to provide a view that will aid South African judicial officers in interpretation and application of cybercrime specific legislation and guide the practical application of investigative methods used in the search and seizure of electronic evidence.

5. Statement of Purpose and Rationale

The purpose of this study is to evaluate the current South African legislation, policies and procedures relating to the search and seizure of electronic evidence in the

[80] GP Bouwer (note 31 above; 163).
[81] Rule 41 (b) (6) of the Federal Rules of Criminal Procedure, 2016.
[82] NY Conteh and PJ Schmick 'Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks' (2016) 6(23) International *Journal of advanced Computer Research* 33.
[83]1914 (Cth). G Urbas and KR Choo 'Resource materials on technology-enabled crime' 2008 *Australian Institute of Criminology* 28.
[84] Section 3K of the Crimes Act 1914 (Cth).
[85] Section 3L of the Crimes Act 1914 (Cth).

investigation of cybercrime and analyse if the enactment of the Cybersecurity and Cybercrimes Bill will address the present shortcomings effectively or whether more insight from international best practices should be considered.

The rationale for this study is based on investigating the difference between the high increase in the rate of cybercrime being committed and its corresponding low conviction rate. One would expect high cybercrime conviction rates in light of the increase in the rate of cybercrime, however, the opposite is evident. It is therefore imperative to study the legal framework and its practical application governing the search and seizure of electronic evidence in the investigation of cybercrime in order to uncover its shortcomings and recommend means of improvement.

In addition, the Cybersecurity and Cybercrimes Bill has not been passed into law as yet therefore it has not yet been subject to judicial interpretation. Neither has it passed constitutional muster. It is advantageous to study this Bill now to predict the effect it will have on all the stakeholders involved in the search and seizure of electronic evidence.

6. Structure of dissertation

Chapter 2 of this dissertation deals with the current regulations governing search and seizure of electronic evidence in South Africa. The collection of the electronic evidence is vital in the successful investigation of cybercrime hence it is important to pay attention to these regulations in light of its practical application, judicial interpretation and economic impact. The main focus of this chapter entails scrutinizing the ECT Act and CPA.

An analysis of the salient provisions of the Cybercrimes and Cybersecurity Bill will be done in this chapter 3. These will be compared to the existing regulatory framework and relevant distinctions will be drawn in an attempt to reveal whether the proposed changes will adequately address the shortcomings of its predecessors. An anticipated limitation is the lack of case law relevant to this topic that can aid in interpretation and application of the law.

Chapter 4 entails an examination of the regulatory frameworks of international and foreign jurisdictions (USA and Australia) in order to conduct a comparative study depicting the areas succeeding and/or lacking in South African law. Considering international best practice will assist in providing recommendations as well as to draw a conclusion on whether South Africa is on par with other nations in terms of its legal development.

The last chapter will conclude this research paper by summarising all arguments and findings presented as well as by providing a thoroughly researched set of recommendations that will assist in developing South African law to meet international standards and improve operating procedures within the country.

7. Research Methodology

The research conducted for this dissertation will be qualitative in the form of desktop research. Legislation such as the Electronic Communications and Transactions Act will be analysed for the current position in South Africa and the Cybercrimes and Cybersecurity Bill will be analysed for the future position together with various other applicable legislation and policies on this topic. Relevant case law, be it reported or unreported judgements, will be looked at to obtain a view of the attitude of the courts toward cybercrime.

Further, literature in the form of published textbooks, journal articles, newspaper and media reports will be utilised as a basis for discussion around the topic as well as to either support or contrast arguments being made. In addition, legislation and journal articles published by legal academics from foreign jurisdictions relating to the search and seizure of electronic evidence will be used to do a comparative study between South Africa and other jurisdictions.

CHAPTER TWO - CURRENT LEGAL POSITION IN SOUTH AFRICAN REGARDING SEARCH AND SEIZURE OF ELECTRONIC EVIDENCE

1. Introduction

Cybercrime is not a new phenomenon to South Africa. Electronic devices and technology such as the internet, cell phones, podcasts, and digital cameras to name a few, are used as a medium of communications, transactions, interactions and the recording of events.[86] With the advancement of technology comes the increased risk of computers becoming either the tools or targets of crime.[87]

This chapter aims to identify and critically analyse the current legal framework that governs the search and seizure of electronic evidence in a criminal context in South Africa. This will be done by evaluating, firstly, the definition of electronic evidence, secondly, a constitutional perspective of search and seizure, and lastly the search and seizure provisions of the relevant legislation. In addition, relevant judicial decisions will be considered to uncover the interpretation of the applicable law, and its practical application and impact.

2. Defining electronic evidence

2.1. Overview

This increase in the use of technology has resulted in the creation of new laws depicting the criminal law's reaction to this change in social conditions.[88] In South Africa, the law of evidence is not codified in a single piece of legislation and spans a variety of sources which range from the Civil Proceedings Evidence Act[89] to the Criminal Procedure Act[90] and to the Computer Evidence Act,[91] which has now been

[86] EA Vincze (note 17 above, 186) See also A Bellengere et al… *The Law of Evidence in South Africa: Basic Principles* (2013) 73.
[87] South African Law Commission Discussion Paper 99 (Project 108) 'Computer related crime: Preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects' (2001) 3.
[88] J Omar (note 50 above, 229).
[89] Act 25 of 1965.
[90] Act 51 of 1977.
[91] Act 57 of 1983.

repealed by the most recent, and primary regulator of electronic evidence in South Africa: the Electronic Communications and Transactions Act.[92]

Moreover, electronic evidence does not form part of a *sui generis* category in the South African law of evidence, but is admitted to court as documentary evidence in the form of a document, or real evidence in the form of a thing.[93]

In South African law, the term electronic evidence does not exist – rather, the term *data message* is used in section 1 of the ECT Act reflecting the United Nations Model Law on Electronic Commerce, 1996.[94] It was never the intention of the Model Law to limit the concept of data messages to only means of communication but rather include all kinds of messages that are 'generated, stored or communicated' in electronic form inclusive of computer records.'[95]

Nevertheless, electronic evidence has also been defined as 'information of probative force stored or transmitted in digital format'[96] or as 'electronically stored information that can be used as evidence in a legal action.'[97] Examples of electronic evidence that can be admitted into evidence at a trial are images and sound extracted from a cell phone.[98] Further computer evidence, digital video, digital fax machines and digital audio are all classified as electronic evidence.[99]

Similarly, Nieman sets forth two different types of electronic evidence, one being physical and the other being logical.[100] Physical electronic evidence is described as

---

[92] A Bellengere et al (note 87 above, 73). This is seen as problematic which is duly noted by the SA Law Reform Commission to be discussed later on in this paper.
[93] PJ Schwikkard and SE van der Merwe (note 43 above, 438).
[94] This definition is based on the definition of 'data message' provided for in Article 2 of the Model Law to be further described in paragraph 2.3.1 of this Chapter. See S Papadopoulos (note 7 above, 319).
[95] South African Law Reform Commission, Issue Paper 27, Project 126: Review of the Law of Evidence. Electronic evidence in criminal and civil proceedings: admissibility and related issues (accessed through *http://salawreform.justice.gov.za/ipapers/ip27_pr126_2010.pdf* on 2 July 2017).
[96] GP Bouwer (note 31 above, 159).
[97] P Volonino 'Electronic evidence and computer forensics' 2003 *Communication of the Association for Information Systems* 462.
[98] *Motata v Nair No and Another* 2009 (1) SACR 263 (T).
[99] Y Shin 'New Model for Cyber Crime Investigation Procedure' 2011 (2) *Journal of Next Generation Information Technology* 1.
[100] A Nieman *Search And Seizure, Production And Preservation Of Electronic Evidence* (unpublished LLD Thesis, North-West University, 2006) 36.

machinery and hard drives, whereas logical electronic evidence is said to live within log files and is embedded in memory and software.[101]

Mason and Seng propose that the definition of electronic evidence comprises of three different elements.[102] Firstly, data which 'includes all forms of evidence created, manipulated or stored in a device that can, in its widest meaning, be considered a computer.'[103] Secondly, it refers to various devices that can store or transmit data such as computers or telephone systems.[104] Lastly, the definition restricts data to that which is relevant to the case at hand when deciding on the admissibility of the electronic evidence.[105]

The above definitional issues notwithstanding, the admissibility of electronic evidence is not central to the theme of this paper but with the aim of completeness it is beneficial to note that the admissibility of *any* evidence is based on its relevance to the facts at issue.[106] Admissibility is further dependent on whether or not the evidence may be excluded by any other law, or precluded due to the manner in which it was obtained.[107] One ultimately analyses the probative value and relevance of the evidence – while considering whether the evidence may cause prejudice to one or more parties at trial.[108] Each case is decided on its own merits, and the judicial officer will ultimately decide whether evidence is admissible or not.[109]

2.2. Electronic evidence – civil

As noted above, the ECT Act attempts to define electronic evidence[110] by defining data as the 'electronic representations of information in any form'.[111] It further defines a "data message" as 'data generated, sent received or stored by electronic means and

[101] *Ibid.*
[102] S Mason and D Seng *Electronic Evidence* 4ed (2017) 19.
[103] *Ibid.*
[104] *Ibid*, 20.
[105] *Ibid.*
[106] *R v Trupedo* 1920 AD 58 at 62.
[107] PJ Schwikkard (note 43 above, 438).
[108] *Ibid.*
[109] *Ibid*.
[110] PJ Schwikkard 'Evidence' 2003 *SACJ* 90.
[111] Section 1 of the ECT Act.

includes voice, where the voice is used in an automated transaction; and a stored record.'[112]

Zeffertt is of the view that the ECT Act aimed to provide for the admissibility of information or data arising from electronic communications transactions.[113] Therefore, from the perspective of the admissibility of electronic evidence, rules that apply to both documentary and real evidence are applicable.[114]

2.3. Electronic evidence – criminal

From a criminal law perspective, electronic evidence is regulated under the CPA which makes provision for a document, which 'includes any device whereby information can be recorded or stored.'[115] This provision places a limitation of the extent to which electronic evidence could be covered as a document in the CPA by only making reference to the functionality of recording and storing. Early interpretations of a "document" did not include computers as the operational functionality of a computer exceeded recording and storage of information.[116] However, the courts have decided that computer print-outs fall within the ordinary meaning of a document as they consist of typed words and figures thus leading to the admissibility of computer print-outs in criminal proceedings.[117]

In addition, in the case of *S v Brown,*[118] the court held that photographic images that were downloaded from a mobile phone and in general 'generated, stored and transmitted by an electronic device' should be dealt with as documentary evidence as opposed to real evidence. Even though this case does not directly deal with the definition of electronic evidence, it illustrates that electronic evidence has been admitted into court in criminal proceedings through the CPA.

---

[112] *Ibid.*
[113] DT Zeffert et al *The South African Law of Evidence* (2003) 699.
[114] *Ibid.*
[115] Section 221(5) of the CPA.
[116] J Hofman 'Electronic evidence in criminal cases' (2006) 19 South African Computer Journal 257.
[117] *S v Harper* 1981 (1) SA 88 (D). See also *S v Ningisa and Others* 2013 (2) NR 504 (SC).
[118] 2016 (1) SACR 206 (WCC).

2.4. Conclusion regarding the current definition of electronic evidence

The concept of electronic evidence has no standard definition. This is required in order to achieve fairness and consistency. Therefore, it is submitted that the definition of electronic evidence should be standardised and defined by law in order to mitigate against any misunderstanding and contradictory interpretations. This is important because, as noted above, electronic evidence forms part of all areas of law therefore it should be defined uniformly across the board. With the introduction of the Bill, South African legislation may get closer to defining electronic evidence.[119]

3. Search and Seizure of electronic evidence: current legal position

3.1. The Constitution of the Republic of South Africa, 1996

The introduction of the Constitution brought about restrictions onto search and seizure powers, prescribing standards which legal powers are measured against.[120] However, section 36 of the Constitution provides that these rights are subject to reasonable and justifiable limitations that are imposed by a law of general application.[121] Certain constitutional aspects are discussed below in the context of search and seizure of electronic evidence within the cyber-realm.

3.1.1. The right to a fair trial

Section 35 (3)(j) of the Constitution reads:

> Every accused person has a right to a fair trial, which includes the right not to be compelled to give self-incriminating evidence

The right to a fair trial and the privilege against self-incrimination[122] is provided by both the Constitution, and the CPA which provides that 'no witness shall… be compelled to answer any question which he would have not … have been compelled to answer by

[119] This will be discussed further in the next chapter.
[120] V Basdeo (note 41 above, 307).
[121] *Ibid.*
[122] *Ibid.*

reason that the answer will expose him to a criminal charge.'[123] The right to silence is an underpinning mechanism that supports the concept of personal liberty.[124]

With technological tools such as password encryption and security features on devices, the simplest method that investigators can use to gain access to locked information is to compel the individual who possesses or controls the access to comply with their investigation.[125]

Investigations that do not comply with constitutional mandates bear the risk of the loss of evidence for purposes of prosecution and possible liability on part of the police.[126] From a constitutional perspective, evidence should be excluded if such evidence was obtained in a way that violates a constitutional right and if the admission of such evidence would render a trial unfair.[127] However, the admissibility of evidence, albeit collected in an unlawful manner, should be adjudicated upon by a trial court.[128]

3.1.2. The right to privacy

Section 14 reads:

> Everyone has the right to privacy, which includes the right not to have their person or home searched; their property searched; their possessions seized; or the privacy of their communications infringed.[129]

This is a fundamental human right that is afforded to every citizen of South Africa yet these rights impose limitations on the powers of search and seizure.[130] Search and seizure is deemed to infringe on an individual's right to privacy, dignity, freedom, security and property. Therefore this procedure must be carried out lawfully under the

[123] Section 203 of the CPA.
[124] Hiemstra (note 59 above, 10).
[125] C Theophilopoulos 'Electronic documents, encryption, cloud storage and the privilege against self-incrimination' 2015 *South African Law Journal* 597.
[126] V Basdeo (note 45 above, 153).
[127] CG van der Merwe and JE du Plessis (ed) *Introduction to the Law of South Africa* (2004) 519.
[128] *Zuma v National Director of Public Prosecutions* 2008 (2) SACR 421 (CC). See also Harvey v Niland 2016 (2) SA 436 (ECG).
[129] Section 14 of the Constitution.
[130] VM Basdeo et al 'Search and seizure of evidence in cyber environments: a law enforcement dilemma in South African criminal procedure' (2014)1 Journal of Law, Society and Development 48-67.

guidance of a warrant[131] and within the restrictions of the Act to avoid the question of whether a search was unlawful and constitutes an infringement of privacy.[132]

In the case of *Harvey v Niland*[133] the court accepted that Niland's Facebook communications were acquired unlawfully as Harvey hacked into the Niland's Facebook account to gain access to his communications. The court held that this constituted a violation of Niland's privacy. However, the court held that the admission of the electronic evidence depended on, *inter alia*, the extent to which the right to privacy was infringed and whether there was a lawful means to obtain the evidence.

3.2. The Common Law

In South Africa, the law of evidence is governed by both statutory law and common law.[134] An example of the common law is set out in the case of *Ex Parte Minister of Justice: In re R v Matemba*[135] which states that 'production of documents by a person in response to a subpoena… or to other forms of process treating him as a witness… may be refused under the protection of the privilege.'[136]

In terms of criminal proceedings, before the promulgation of the ECT Act, cybercrime was dealt with under the common law.[137] One such example of the application hereof was the case of *S v Van den Berg.*[138] In this matter, the court found that misrepresentation via a computer system (electronically) amounted to the same conduct as making a false handwritten entry into a ledger account via traditional means and the accused was convicted of fraud.

---

[131] V Basdeo 'A constitutional perspective of police powers of search and seizure: The legal dilemma of warrantless searches and seizures' (2009) 3 South African Journal of Criminal Justice 404.
[132] VG Hiemstra (note 59 above, 7).
[133] 2016 (2) SA 436 (ECG).
[134] M Watney (note 39 above, 2).
[135] 1941 AD 75 at 81.
[136] C Theophilopoulos (note 125 above, 603).
[137] S Snail 'Cyber Crime in South Africa – Hacking, cracking, and other unlawful online activities', 2009(1) *JILT* 2.
[138] *S v. Van den Berg* 1991 (1) SACR 104 (T).

In 1999, the court faced a decision in the case of *S v Howard*[139] on whether the loading of a malicious code into a computer network system amounted to the common law crime of malicious injury to property.[140] Ultimately, the court held that such crime did apply to data messages and information, and the accused was accordingly convicted and sentenced to five years imprisonment.[141]

3.3. Criminal Procedure Act 51 of 1977

3.3.1. Introduction

Chapter 2 of the CPA contains the search and seizure provisions in criminal procedure. It provides the legal basis for acquiring warrants for search and seizure and the actions to perform in the absence of a warrant.[142] As a condition, under chapter 2, search and seizure captures the principle that 'there must be a reasonable belief that a certain article located, on a particular premises is connected with the commission of an offence.'[143]

However, the South African Law Commission concluded, in the year 2000, that the CPA was designed for the investigation of the physical world and search and seizure of physical evidence.[144] It appears that the most apparent challenge that the search and seizure of electronic evidence poses for the application of the CPA is that this piece of legislation was created for a physical world where the seizure of evidence related to tangible objects – in tangible places. Computer-generated evidence in the realm of cyberspace was not envisaged. [145]

The procedure involved in the search and seizure of electronic evidence entails firstly, searching for and seizing the physical electronic equipment (e.g. computers and hard drives) that may contain potential evidence, and secondly, searching the physical

[139] Unreported Case no. 41/ 258 / 02, Johannesburg Regional Magistrates Court.
[140] *Ibid.*
[141] *Ibid.*
[142] V Basdeo (note 130 above). The ECT Act also provides for cyber inspectors to apply for warrants however, these provisions were never realised as the cyber inspector was never appointed to implement same. Further discussed in paragraph 2.3.2 of this chapter.
[143] V Basdeo (note 131 above, 405).
[144] South African Law Commission Discussion Paper 99 (note 87 above, 13).
[145] GP Bouwer (note 31 above, 157).

electronic equipment and seizing the evidence located therein.[146] It is noted that the provisions of the CPA can be applied to the first search and seizure of physical evidence.[147]

It is submitted that the provision, however, does not apply to the second search of the physical evidence and the seizure of the contents located therein as this would then require an application for a second warrant or the details of the second search to be identified in the initial warrant.[148] Consequently, this second search may be unlawful as it constitutes hacking as defined by section 86 of the ECT Act.[149] This is one of the issues with the current legislation and as such legislative intervention in the form of providing specific procedures is required to ensure that the search of the seized physical electronic equipment is done lawfully.[150]

Discussed below are the general provisions of the CPA that pertain to search and seizure that govern tangible evidence. Highlighted are the nuances involved in the application of these provisions to the search and seizure of electronic evidence in the investigation of cybercrime.

3.3.2. Search and Seizure provisions and its challenges

(a) Search warrants

General searches and seizures are carried out under the authority of a warrant as prescribed by section 21 of the CPA.[151] Section 21 of the CPA sets out that articles can be seized by virtue of a lawful search warrant which requires police officials to seize the article in question and further authorises the police official to search any person or premises or any person found on the premises identified in the warrant.

---

[146] OS Kerr 'Search warrants in an era of digital evidence: *Symposium: the search and seizure of computers and electronic evidence*' (2005) 75 *Mississippi L J* 85–138.
[147] *S v Miller & others* 2016 (1) SACR 251 (WCC).
[148] Ibid. See also South African Law Commission Discussion Paper 99 (note 87 above) and DP Van der Merwe… et al (note 12 above, 77).
[149] GP Bouwer (note 31 above, 169).
[150] This is discussed in paragraph 2.2.2 (c) of this Chapter.
[151] A Nieman (note 100 above, 159).

The CPA specifically provides for the search by means of a warrant.[152] The following information must be included in a valid search warrant to enable a proper search: identify the searcher; identify the container, premises or person to be searched; describe, with sufficient particularity, the article to be searched for and seized; and the offence that triggered the criminal investigation.[153] This statute provides that an article may only be seized by virtue of a search warrant whereby the person and/or premises to be searched are identified in the search warrant.[154]

It is submitted that currently the second search is conducted by a different searcher and at a different location which details are not set out in the warrant.[155] The second search, therefore, does not fall within the ambit of the initial warrant granted.

The constitutional court set out that vagueness or over breadth in search warrants can be dispelled by defining the scope of the search and confining the actual search and seizure to those articles and premises that are set out in the warrant as having a bearing on the investigation.[156] This practice of not having a broad and general warrant acts as a safeguard against criticism of the warrant.[157]

By way of illustration, in the case of *Zoeco System Managers CC v Minister of Safety and Security N.O.* the applicant sought to set aside a warrant whereby its computer equipment and other electronic devices were seized.[158] Its application was successful, one of the grounds being that the articles to be seized were not described with sufficient particularity therefore the applicants were unable to decipher which articles were susceptible to being searched and seized.[159]

Further, in the case of *Powell N.O v Van der Merwe N.O*[160] the court held that phrases used in the warrant, such as “all documents” and “any other document and/or object that has relevance to or may have relevance to the investigation”, provided vague

[152] Section 21 of the CPA.
[153] A Le Roux-Kemp ‘Criminal Procedure’ (2011) Annual Survey of South African Law.
[154] Section 21 of the CPA.
[155] GP Bouwer (note 31 above, 156).
[156] *Minister of Safety and Security v Van der Merwe and Others* 2011 (2) SACR 301 (CC).
[157] *Ibid.* V Basdeo (note 45 above, 168).
[158] *Zoeco System Managers CC v Minister of Safety and Security No and Others* 2013 (2) SACR 545 (GNP).
[159] *Ibid.*
[160] 2005 (1) SACR 317 (SCA).

guidance as to what can or cannot be seized. The warrant was accordingly set aside.[161]

Courts apply a 'principle of strict interpretation' when dealing with search warrants as portrayed in the *Beheermaatschappij Helling I NV case*[162] where the court held that only the search and seizure of 'documentation' was authorised by the warrants in question and electronic equipment such as CPU's fell outside the ambit of this warrant.[163] However this principle was not always applied as seen in the case of *Seccombe*[164] where the court described a 'document' as a broad term which can include everything consisting written or pictorial proof irrespective of the material that it is made of, thus including electronic information.[165] Further, a document can encompass invisible images on tapes, films, videotapes, flash drives, computer discs or other devices.[166]

Another point to mention is that in instances where the police seize items that are not listed in the search warrant and go beyond the scope of the warrant, the court is not quick to render such a search and seizure as unlawful but prefers to remedy the situation by ordering the return of the items.[167]

This inconsistency depicts a clear legal uncertainty in the interpretation and application of these search and seizure provisions. It is submitted that the lack of particularity in describing the electronic evidence to be seized poses a challenge in the investigation of a cybercrime being in accordance with a search warrant.

(b) Search of premises

In terms of search and seizure the CPA defines 'premises' as 'including land, any building or structure, or any vehicle, conveyance ship, boat or aircraft'.[168] Bouwer

[161] *Ibid.* See also GP Bouwer (note 31 above, 167).
[162] *Beheermaatschappij Helling I NV v Magistrate, Cape* Town 2007 (1) SACR 99 (C).
[163] M Cowling 'Criminal Procedure' 2007 South African Journal of Criminal Justice 351.
[164] *Seccombe v. Attorney-General* 2002 (2) All SA 185.
[165] M Watney (note 39 above, 5).
[166] DS De Villiers 'Old "documents", "videotapes" and new "data messages" – a functional approach to the law of evidence (part 1) (2010) 3 *TSAR* 564.
[167] *Polonyfis v The Minister of Police* (64/2010) [2011] ZASCA 26.
[168] Section 1 of the CPA.

argues that the search of a computer falls outside the ambit of this definition.[169] The South African Law Commission is of same view in that a physical computer may be seized under the provisions of the CPA however the uncertainty lies with obtaining a warrant to search for and seize any electronic evidence contained on the computer.[170] To overcome the above uncertainty in searching for items that are intangible in nature, s 82(4) of the ECT Act provides that the concept of "premises" as referred to by the CPA includes information systems resulting in the inclusion of electronic evidence. The ECT Act defines information systems as 'a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet.[171]

Our court is of the view that the premises should be intelligibly described in the warrant meaning that those officials who are conducting the search are able to identify the premises.[172] An incorrect description of the premises does not render the warrant invalid where sufficient particularity is used when describing the premises.[173] In the writer's view, should a search of a computer or similar electronic equipment be required then the warrant should state the premises as an information system as provided by the ECT Act. However, this opinion is in need of judicial scrutiny as well as input from other experts in the field.

(c) Bouwer's two-step process[174]

Bouwer's two-step process regarding the search and seizure of electronic evidence involves:

- Firstly, searching of a physical environment and seizing of tangible objects. This entails police officials entering the physical premises that is subject to the

[169] GP Bouwer (note 31 above, 158).
[170] South African Law Commission Discussion Paper 99 (Project 108) (note 87 above).
[171] Section 1 of the ECT Act.
[172] *Polonyfis v The Minister of Police* (note 163 above).
[173] *Ibid.*
[174] Gideon Bouwer is an experienced policeman and advocate of the High Court who specialises in information technology law. He has the practical experience of enforcing the law as well as the knowledge of legislative instruments. M Saville 'Cop becomes advocate' *news24 archives* 2006 available at *http://www.news24.com/SouthAfrica/News/Cop-becomes-advocate-20060424,* accessed on 27 August 2017. G Bouwer 'ICT policy proposals spell out an attempt to nationalise assets' *Business Day* 2017 available at *https://www.businesslive.co.za/bd/opinion/2017-03-13-ict-policy-proposals-spell-out-an-attempt-to-nationalise-assets/,* accessed on 27 August 2017.

search and thereafter searching for and seizing the electronic devices (computer hardware and the like); and

- Secondly the searching of seized electronic devices and the seizure of electronic evidence found on those devices. This involves removing the electronic devices from the searched premises and thereafter, at a later stage, searching the electronic device and seizing the electronic evidence located therein.[175]

Consequently, these seizures occur at different times and in different places and are performed by different individuals.[176] However, currently it is viewed as a single process which means that should the search and seizure of the physical equipment be unlawful then the search and seizure of the electronic evidence will follow suit.[177] In previous cases involving electronic evidence, only a single warrant was issued which made references to using forensic analysis to conduct searches "at a location removed from the premises."[178] In light of the above, it is submitted that police officials have two options namely the application for a second warrant or the application of a single warrant that sets out both search and seizure procedures with sufficient detail and particularity to be able to differentiate between the two different procedures.

In the context of electronic evidence, the second step extended the ability to access the contents of the articles that were seized.[179] At times it can be argued that the police do not have the requisite authority that a cyber inspector[180] has to access information contained on seized items therefore the conduct of the police could result in a contravention of s86(1) of the ECT Act being unauthorised access to data.[181]

In the writer's view, the implementation of the two-step process will break ground in the search and seizure of electronic evidence by being procedurally correct and minimising the risk of technicalities being raised in defence. However, the second step

[175] GP Bouwer (note 31 above, 166).
[176] *Ibid.*
[177] *Ibid.* See also *Cadac (Pty) Ltd v Weber-Stephen Products Co* 2011 (3) SA 570 (SCA) at para [18].
[178] *Thint (Pty) Ltd v National Director of Public Prosecutions and Others; Zuma v National Director of Public Prosecutions and Others* 2008 (2) SACR 421 (CC) at para [19]. See also *Van der Merwe v Additional Magistrate, Cape Town;* 2010 (1) SACR 470 (C) at para [121].
[179] E Du Toit (note 64 above, 13).
[180] As mentioned in Chapter 1 and will be further explored within this chapter.
[181] E Du Toit (note 64 above, 13).

could result in a constitutional challenge where the owner of electronic equipment is deprived of possession while the police carry out the search for electronic evidence.[182]

3.4. Electronic Communications and Transactions Act 25 of 2002

3.4.1. Introduction

In South Africa, in the context of electronic evidence, civil proceedings were regulated by the Civil Proceedings Evidence Act[183] and the Computer Evidence Act (CEA).[184] One of the primary academic criticisms levelled against the CEA is that it did not apply to criminal matters and therefore left the regulation of electronic evidence with a lacuna.[185]

Consequently, criminal proceedings were left with no direction, other than the common law[186], until 30 August 2002 when the ECT Act came into operation.[187] Prior to the ECT Act, the CPA was the only legal instrument that governed electronic evidence in criminal matters through sections 221 and 222.[188] The ECT Act is a mechanism that government used to establish a structure to regulate and define e-commerce in South Africa.[189]

However, this not does mean that all other laws are no longer applicable as Section 3 of the ECT Act states:

> 'This Act must not be interpreted so as to exclude any statutory law or common law from being applied to, recognising or accommodating electronic transactions, data messages or any other matter provided for in this Act.'[190]

---

[182] *Beheermaatschappij Helling I NV v Magistrate, Cape Town* (note 158 above).
[183] Act 25 of 1965
[184] Act 32 of 1985. The requirements of this Act were overly technical in nature resulting in difficulty in compliance. The Act was accordingly repealed by the ECT Act and this repeal was welcomed. PJ Schwikkard and Van der Merwe (note 43 above, 439).
[185] DP Van der Merwe … et al (note 12 above, 110).
[186] As explained in paragraph 3.2 above.
[187] M Watney (note 39 above, 3).
[188] DP Van der Merwe … et al (note 12 above, 110). Section 221 deals with the admissibility of certain business or trade records and section 222 states that the Civil Proceedings Evidence Act applies *mutatis mutandis* to criminal proceedings.
[189] S Sissing and J Prinsloo 'Contextualising the phenomenon of cyber stalking and protection from harassment in South Africa' (2013)26(2) *Acta Criminologica: Southern African Journal of Criminology* 23.
[190] Section 3 of the ECT Act.

The ECT Act aims to bring about legal certainty regarding electronic communications and transactions[191] and satisfied the obligation which the Cybercrime Convention imposed on its member states to criminalise certain types of electronic conduct. [192]

In aid of bringing the CPA into the virtual realm, the ECT Act provides clarity to the terms 'premises' and 'article' used in the CPA by stating that these terms include information systems and data messages.[193] It therefore makes the CPA applicable to the search and seizure of electronic evidence.

In the investigation of the cybercrimes created by the ECT Act[194] the following evidence will be encountered: computer systems comprising of hard drives, keyboards, monitors, laptops, servers; traditional telephone systems, the internet, wireless telecommunication systems; embedded computer systems which include mobile devices, navigation systems, smart cards, sensing and diagnostic modules, amongst others.[195]

3.4.2. Issues with the search and seizure provisions of the ECT Act.

Firstly, cyber policing was created by the ECT Act by means of introducing the role of a cyber inspector who was meant to be an employee of the Department of Communications.[196] The Act empowers cyber inspectors to search (enter any premises) and seize (access information) that may have an impact on the investigation into cybercrime[197] and further permits the SAPS to call upon the cyber inspector for help in the investigation of a cybercrime.[198]

---

[191] Section 2(e) of the ECT Act.
[192] DP Van der Merwe *Computers and the Law* 2ed 2000 67.
[193] S Papadopoulos et al*.* (note 7 above, 328).
[194] Section 86 and Section 87.
[195] E Casey *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 3 ed (2011) 8.
[196] SL Gereda 'The Electronic Communications and Transactions Act' 2006 *Telecommunications Law in South Africa* 281*.*
[197] F Cassim 'Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study' 2009 (12) *PER* 59*.*
[198] Section 81 (2) of the ECT Act.

The challenge that has been identified in this research is that the ECT Act created the role of a cyber inspector yet none have been appointed.[199] Juxtaposed to chapter 2 of the CPA, s82 of the ECT Act provides a far more detailed account of what the search and seizure of electronic evidence should entail by providing cyber inspectors with these specific powers.

The ECT Act further enables cyber inspectors with more technical search and seizure procedures by affording them the power to monitor and investigate the conduct and activities of a cryptography service provider[200] and an authentication service provider[201] and perform an audit on a critical database administrator.[202]

The current position with regard to this detailed procedure is that it is futile in the sense that no person has been appointed in the capacity of a cyber inspector who would have the skills to carry out these procedures. However, the Act falls short in not specifying the type of qualification a cyber inspector should possess but instead assigns the onus of appointing a cyber inspector to the director-general of the Department of Communications.[203]

Van der Merwe is of the view that even though the ECT Act aimed to bring new developments to the field of investigation into technology and cybercrime, it did not follow through in practical application as no cyber inspectors were appointed.[204] In the writer's view, cyber inspectors were expected to be experts in this specialised field of ICT forensics with their role created to have elevated investigative procedures.

It is submitted that the disadvantage that South Africa has in this regard is that as a result of no cyber inspectors being appointed, the SAPS had no opportunity to seek advanced assistance in the search and seizure of electronic evidence. The SAPS is tasked to investigate cybercrime using the provisions of the CPA which was not

[199] *S v Miller* [2015] 4 All SA 503 (WCC) at para 56. See also S Papadopoulos et al. (note 7 above, 328).
[200] Section 81 (1) (b) of the ECT Act.
[201] Section 81 (1) (c) of the ECT Act.
[202] Section 81 (1) (d) of the ECT Act.
[203] SL Gereda (note 195 above, 281).
[204] DP Van der Merwe… et al (note 12 above, 86).

created to be exercised in the virtual realm without having the status of a cyber inspector and practically applying the below provisions of the ECT Act.[205]

Firstly, cyber inspectors are empowered to:

- Search premises or information systems;[206]
- Search any person on those premises on a reasonable belief that such person is in possession of evidence that can be used in the investigation;[207]
- Inspect facilities on the premises linked or associated with the information system that have a bearing on the investigation;[208] and
- 'have access to and inspect the operation of any computer forming part of an information system and any associated apparatus or material which the cyber inspector has reasonable cause to suspect is or has been used in connection with any offence.'[209]

As seen above these provisions are more technical in nature and cater for the electronic environment. These specialised procedures were never implemented nor practiced.

Secondly, the ECT Act makes provision for cyber inspectors to request a warrant in the investigation of a crime.[210] Such warrant permits their entry into premises and the access of information systems and enables the carrying out of necessary searches in accordance with the provisions set out the ECT Act.[211] The ECT Act warrant differs from the CPA warrant in that it does not make reference to a peace officer and the warrant must specify 'the premises or information system' that search and seizure applied to.[212] Here, the inclusion of 'information system' remedied the uncertainty surrounding whether it was included in the term 'premises' as set out by the CPA.

[205] V Basdeo 'A constitutional perspective of police powers of search and seizure in the criminal justice system' (unpublished LLM Thesis, University of South Africa, 2009, 139).
[206] Section 81 (1) (a) of the ECT Act.
[207] Section 81 (1) (b) of the ECT Act.
[208] Section 81 (1) (e) of the ECT Act.
[209] Section 81 (1) (f) of the ECT Act.
[210] Section 83 of the ECT Act.
[211] DP Van der Merwe… et al (note 12 above, 86).
[212] Section 83 (3) (a) of the ECT Act. See also V Basdeo (note 65 above, 207).

Thirdly, the legislature through s82 (1) (f) gave authority to cyber inspectors to carry out a search and seizure even if such activity is not stated in the warrant by making reference to 'any offence'.[213] This could apply in a situation where a cyber inspector may whilst executing a search in terms of a warrant, formulates a reasonable suspicion that computer equipment present on the premises has been or is being used in the commission of another offence.[214]

Another difference between the search and seizure provisions of the CPA and the ECT Act is that the ECT Act makes provision for the taking of extracts from or making copies of books, documents, records or information systems; accessing and inspecting the operation of any computer or information system related equipment or any associated apparatus that a cyber inspector reasonably suspects is involved in the commission of a crime.[215]

It is submitted that these provisions are technology driven and requires insight into this field in order to carry out procedures such as being able to identify items that could be used in the commission of a crime. Further the evidential weight allocated to a data message, for instance, is dependent on factors which include 'the reliability of the manner in which the integrity of the data message was maintained.'[216] Therefore it is submitted that the validity of search and seizure procedures of electronic evidence is of utmost importance in prosecution to avoid vital evidence being rendered inadmissible in court.

Lastly, in terms of s82 (2) 'a person who refuses to co-operate or hinders a person conducting a lawful search and seizure in terms of this section is guilty of an offence'. This provision is said to be ambiguous in that it does not explain what constitutes hindering or refusing to co-operate.[217] It is argued that these provisions are inflexible and deficient lacking the attention to privacy and other constitutional concerns as well as the seizure of electronic documents.[218]

---

[213] V Basdeo (note 65 above, 207).
[214] *Ibid.*
[215] Section 82 of the ECT Act and DP Van der Merwe… et al (note 12 above, 86).
[216] S15 (3) of the ECT Act and A Bellengere et al… (note 87 above, 76).
[217] C Theophilopoulos (note 125 above, 597).
[218] *Ibid.*

Another view is that this section was aimed at instances where the information system is password-protected and accordingly the access is denied.[219] Here the cyber inspector is empowered by this provision to compel a suspect to co-operate by providing the password and hence making the data on the information system available to the cyber inspector.[220]

Another prominent challenge that presents itself is that of jurisdiction whereby electronic evidence can be stored on or transmitted from electronic devices outside South Africa territory.[221] In this regard the need for international cooperation and mutual assistance arises.[222]

In light of the above, the current legal position regarding the ECT Act, in the opinion of the writer, is inadequate. In summary, the reasons for the inadequacy is that even though this law is geared towards electronic evidence and devices, the cyber inspectorate which should have the authority to rule in the cyber realm has not materialised. This has left the investigative provisions of the ECT Act dormant and ineffective.

4. Conclusion

Both the ECT Act and the CPA are unable to accurately and effectively deal with or regulate the cyber environment and the current types and levels of cybercrime.[223] This is as a result of the ECT Act's cyber inspectorate not materialising and the lack of cyber specific procedures catered for in the CPA. It is however, acknowledged that the CPA is currently being applied to the search and seizure of electronic evidence. However, the lack of successful prosecutions imply that the provisions of the CPA are not adequately equipped to deal with the nature of cyberspace.

Therefore there is a need to review and update the necessary legislation to adequately deal with the ever-changing nature of technology.[224] It is imperative to take into

[219] DP Van der Merwe… et al (note 12 above, 86).
[220] *Ibid.*
[221] A Bellengere et al… (note 87 above, 78).
[222] *Ibid.*
[223] Irons and Ophoff (note 38 above, 277).
[224] *Ibid.*

account international best practice and the future Cybercrimes and Cybersecurity Bill to make an adequate assessment of the position of South Africa in the investigation of cybercrime.

It is vital that any law enforcement agency, that aim to successfully deal with cybercrime, possesses a basic knowledge and understanding of cyberspace in light of the intricateness and complexity of its nature.[225] In 2014 the Head of the Electronic Crime Unit at the SAPS said 'there is still a widespread ignorance amongst law enforcement officials in the gathering of digital evidence' and emphasised the need for specialised upskilling to 'search, seize, secure (acquisition) and protect the evidential integrity of digital evidence.'[226]

It is submitted that South Africa cannot effectively address the problem of cybercrime as it lacks the necessary legal procedures and/or legal tools.[227] However, in the absence of cyber inspectors, it is submitted that the investigation of cybercrime should not suffer at the worst degree as the SAPS (undergoing the training mentioned above) and various cybersecurity experts in the business sector have the capability to apply electronic forensic principles in the search and seizure process.[228]

Furthermore, there is a growing need for cybercrime specific legislation to overcome the technical difficulties experienced and to provide for the use of electronic evidence in criminal cases[229] and research to be done in a more extensive and in-depth manner on every aspect of cybercrime to aid investigation and prosecution of cyber criminals.[230] It is still to be determined whether the Cybercrimes and Cybersecurity Bill[231] will bring such legislative relief.

---

[225] A Minnaar 'How organised is cybercrime and can it be called organised crime per se?' (2015) 3 (28) *Acta Criminologica: Southern African Journal of Criminology* ii.
[226] L Mashiloane 'Piet Pieterse: SAPS intensifies cyber crime battle' 2014 available at *http://www.itweb.co.za/index.php?option=com_content&view=article&id=134890* accessed on 10 August 2017.
[227] C Theophilopoulos (note 125 above, 596).
[228] J Hofman (note 179 above, 257).
[229] South African Law Reform Commission, Issue Paper 27, Project 126 (note 95 above).
[230] A Minnaar (note 224 above. v).
[231] The Bill is discussed in further detail in Chapter 3 of this dissertation.

CHAPTER THREE - THE CYBERCRIMES AND CYBERSECURITY BILL

1. Introduction and Development of the Bill

On 1 March 2015, South Africa held a Cybersecurity Symposium in which the government acknowledged and addressed the threat that cybercrime poses to South Africa.[232] The Minister of State Security in his speech at the symposium alluded to the fact that the implementation of the ECT Act improved South Africa's legal system to deal with cyber threats.[233] In closing his address the Minister positioned the development of a draft Bill by the Department of Justice and Constitutional Development and further encouraged industry and the public to engage and provide input into its development.[234]

In August 2015 the Department of Justice and Constitutional Development invited comments on the Draft Cybercrimes and Cybersecurity Bill.[235] This 2015 version of the Bill aimed to inter alia, create offences, prescribe penalties and further regulate the powers to investigate, search and gain access to or seize items.[236] One of the criticisms that the 2015 version of the Bill faced was that the definition of "investigator" was too broad and allowed individuals to be appointed that did not have the obligation to adhere to the constitutional and legislative provisions that governed the members of security services.[237]

After the consideration of all comments received, the Department of Justice and Constitutional Development published a notice in the Government Gazette introducing

---

[232] D Mahlobo MP, Minister of State Security 'Remarks on Cybersecurity Symposium' 1 March 2015 available at *http://www.gov.za/speeches/minister-david-mahlobo-cybersecurity-symposium-1-mar-2015-0000,* accessed on 5 April 2017.
[233] *Ibid.*
[234] *Ibid.*
[235] Department of Justice and Constitutional Development 'Cybercrimes Bill Released for Comment' (note 5 above).
[236] *Ibid.*
[237] Adv J Kruger 'Concise Submission on the Draft Cybercrimes and Cybersecurity Bill [B-2015]' 26 November 2015 available *at https://www.ellipsis.co.za/wp-content/uploads/2015/11/151126_cfcr_submission_on_cybercrimes_and_cybersecurity_bill.pdf*, accessed on 30 September 2017.

the Cybercrimes and Cybersecurity Bill, 2017.[238] The current 2017 version is said to be better thought through than its predecessors.[239]

The Bill is viewed as an impetus driving a higher level of cyber security awareness in the business industry and within the government.[240] It has the potential to build and stimulate a vigorous cyber security stance in South Africa however the delays in enacting the legislation is seen as a hampering these efforts.[241]

This chapter aims to review the Bill in light of search and seizure of electronic evidence by commenting on whether it will amend the current position[242] and bringing to light any deficiencies that may still exist.

2. Comparison of the Search and seizure provisions set out in the Bill to the current legal position

Chapter 5 of the Bill sets out the powers to investigate, search and access or seize. This paper will focus on those provisions that attempt to change the current legal position governing search and seizure of electronic evidence. The Bill sets out that the provisions of the CPA apply in addition to the Bill, provided that the CPA is not inconsistent with the provisions of the Bill, in which event, the Bill prevails.[243] Therefore the provisions of the Bill and the CPA apply jointly to the search and seizure of electronic evidence.

2.1 Definitions

The definitions of search and seizure, as set out in the Bill, bring South African cyber-related legislation into alignment with technological developments. The proposed

[238] GN 871 of GG 40487, 9/12/2016; 4.
[239] L Pierce 'Cybercrimes Bill – much better in 2017' IT – Online available at https://it-online.co.za/2017/01/25/cybercrimes-bill-much-better-in-2017/, accessed on 3 June 2017.
[240] K Doyle 'Data breaches remain unreported by SA organisation' 15 March 2017 *ITWeb Security* available at *http://www.itweb.co.za/index.php?option=com_content&view=article&id=160221:Data-breaches-remain-unreported-by-SA-organisations&catid=234,* accessed on 16 September 2017.
[241] *Ibid.*
[242] The current legal position is discussed in Chapter 2 of this research paper.
[243] Section 25 of the Bill.

definitions now include databases, devices and computer networks - these concepts are central to the search and seizure of electronic evidence.[244]

This adds to and amplifies the current legal position of the CPA which did not expressly specify that its application extended to cyberspace.[245] The impact of this change is that it brings about legal certainty by providing for specific definitions that are involved in the search and seizure of electronic evidence.

In comparison to the ECT Act, the concept of electronic evidence was limited to the terms “data’ and “data message” however it broadened the term premises used in the CPA to include information systems.[246] The Bill expands on the foundation set by the ECT ACT by detailing different types of electronic devices and mediums such as programmes, systems, and storage mediums as depicted below.

With specific regard to search and seizure of electronic evidence the Bill now introduces the term “access” which is defined as:

> for purposes of Chapter 5, includes without limitation to make use of data, a computer program, a computer data storage medium or a computer system or their accessories or components or any part thereof or any ancillary device or component to the extent necessary to search for and seize an article.

One of the salient new features of the Bill in relation to the investigation of electronic evidence is that the concept “seize” is now defined as including the following:

> (a) remove a computer data storage medium or any part of a computer system;
> (b) render inaccessible data, a computer program, a computer data storage medium or any part of a computer system in order to preserve evidence;
> (c) make and retain a copy of data or a computer program; or
> (d) make and retain a printout of output of data or a computer program.[247]

Further to the definition of “seize” the Bill defines an “article” as:

> any data, computer program, computer data storage medium, or computer system which—

[244] M Musoni (note 232 above, 689).
[245] *Ibid.*
[246] As discussed in Chapter 2 in this research paper.
[247] Section 1 of the Bill.

(a) is concerned with, connected with or is, on reasonable grounds, believed to be concerned with or connected with the commission or suspected commission;
(b) may afford evidence of the commission or suspected commission; or
(c) is intended to be used or is, on reasonable grounds, believed to be intended to be used in the commission,
of an offence in terms of Chapter 2 or section 16, 17 or 18 of the Act or any other offence which may be committed by means of or facilitated through, the use of such an article, whether within the Republic or elsewhere.

However, the Bill sets out that the CPA still applies together with the provisions set out in the Bill as long as they do not contradict each other.[248] The impact of introducing definitions that cater for electronic devices, in addition to providing consistency and clarity to the existing legal position, is that it educates police officials with the knowledge that there are different types of electronic devices which have the capacity to create and store data in electronic form, and such data may constitute evidential material.[249] It further equips attorneys to be aware that there are various electronic devices that electronic evidence can be retrieved from and advise their clients on investigation, admissibility, disclosure and treatment of electronic evidence.[250] These examples show that the promulgation of the Bill will bring about a greater sense of awareness and competency in those that deal with challenges involving technology.

It is submitted that the Bill does not necessarily change the existing regulations of the CPA but brings about much needed cyber specific provisions and legislation that directly address the search and seizure of electronic evidence. In this regard, should the Bill be promulgated, it would result in South Africa taking a step forward in aligning with the advancement of technology. Further, it is anticipated that law enforcement and prosecution will be equipped to secure not only cybercrime convictions but also be able to gather data that can serve as evidence in the prosecution of other crimes and aid in legal matters.

[248] Section 25 of the Bill.
[249] S Mason and D Seng (note 103 above, 1).
[250] *Ibid,* 17.

2.2. Standard Operating Procedures[251]

Chapter 5 of the Bill starts with an introduction into standard operating procedures being developed that must be observed by the SAPS or any other authorised investigator when carrying out any investigation in relation to the offences set out by the Bill.[252] The standard operating procedures should be issued within six months of the commencement of this Chapter.[253] The standard operating procedure becomes operative when the relevant authority in the Department that is responsible for authorising it signs the document.[254]

The standard operating procedures will be of great benefit in the search and seizure of electronic evidence in that it will standardise the activities that occur in an investigation, it will set out the expectations of the applicable personnel and it can serve as a framework for training.[255] The standard operating procedures sets the Bill apart from the current legal position as it provides for a set of written instructions that will inform the routine or activities that the SAPS will engage in when conducting an investigation.[256]

It is evident that the drafting of the Bill was influenced by the Cybercrime Convention, in that the Cybercrime Convention provides that "legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings."[257] It is submitted that the standard operating procedures speak to the specific criminal investigations mentioned in the Cybercrime Convention.

---

[251] Standard Operating Procedures "is a specific procedure or set of procedures established to be followed in carrying out a given operation or in a given situation to enhance quality through following a standardardised work procedure." The Department: Public Service and Administration 'Toolkit on Standard Operating Procedures' available at *http://www.dpsa.gov.za/dpsa2g/documents/tenders/DPSA002_2015/TOOLKIT%20ON%20STANDARD%20OPERATING%20PROCEDURES%20march%202013.pdf*, accessed on 28 September 2017.
[252] Section 24 of the Bill.
[253] Section 24 of the Bill.
[254] The Department: Public Service and Administration 'Toolkit on Standard Operating Procedures' See note 258 above.
[255] *Ibid.*
[256] *Ibid.*
[257] Article 14 of Council of Europe Convention on Cybercrime European Treaty Series (note 76 above).

As the investigation of electronic evidence is a developing field, it is recommended that a framework of standards governing the process of search and seizure of electronic evidence be prioritised and drafted.[258] The legislature took this approach when law enforcement was confronted with the collection of other evidence that required forensic analysis such as DNA. To this end the Criminal Law (Forensic Procedures) Act[259] together with its corresponding regulations[260] were enacted as provision for DNA customised guidelines. In the same light electronic evidence specific guidelines should be established. South Africa can draw guidance and insight from international institutions such as, inter alia, INTERPOL and the International Organisation on Computer Evidence, when drafting these Standard Operating Procedures.[261]

The drafting of Standard Operating Procedures has been delegated to knowledgeable individuals that are essentially subject matter experts in the field and actually carry out the duties and related procedures.[262] Currently, there appears to be Interim Standing Operating Procedures Dealing with Electronic Evidence and a Practical Guide to Apply for Search Warrants in terms of the Provisions of Section 21 of the Criminal Procedure Act which will aid the formalisation of a final standard operating procedure.[263] It is reported that the Interim Standing Operating Procedures define electronic devices, provide for digital forensic investigators and specificity in a warrant of whether or not copies of data will be made on-site or off-site.[264]

This may result in the drafting of the final standard operating procedures occurring sooner rather than later. However, it is hoped that this can be accomplished within the designated six month period with due regards to the technical nature of electronic evidence, the lack of expert human resources that are currently operating in this field and the due process of reviewing and approval of the standard operating procedures.

---

[258] S Mason *Electronic Evidence* 3ed (2012) 73.
[259] Act 37 of 2013.
[260] Forensic DNA Regulations, 2015. Government Gazette No. R. 207. 13 March 2015.
[261] Expanded on in Chapter 4 of this paper.
[262] The Department: Public Service and Administration 'Toolkit on Standard Operating Procedures' See note 258 above.
[263] DC Myburgh 'Developing a framework for the search and seizure of digital evidence by forensic investigators in South Africa' (unpublished Magister Commercii in Forensic Accountancy thesis, 2016) 61. The documents cited in this paper could not be sourced as it is not publicly available information, therefore the contents thereof could not be reviewed and confirmed.
[264] *Ibid, 61, 81 and 116.*

The full effect of the (search and seizure provisions) Bill will not be realised until such time that the standard operating procedures are put in place.

2.3. Cyber inspector vs police official

As detailed in the previous chapter, one of the main inadequacies of the current legal position is the lack of manifestation of the cyber inspector. The most glaring and obvious difference between the Bill and the current legal position is that the Bill does not mention or cater for the cyber inspector. It is submitted that this is possibly due to a cyber inspector not ever materialising.[265]

In the fifteen years that the ECT Act has been effective, the SAPS attempted to carry out the functions that were specifically created for the cyber inspector. As a result, the Bill now moves away from creating a new ideal persona to reign over search and seizure of electronic evidence and adds this role to the already existing search and seizure powers of the police.

The Bill now refers to police officials making written application for a search warrant and being identified in the warrant whereas the ECT Act provided for cyber inspectors.[266] In addition to a police official, an investigator or any other person may be required to assist the police official by the warrant.[267] An investigator, is defined in the Bill as:

> any person, who is not a member of the South African Police Service and who is—
> *(a)* identified and authorised in terms of a search warrant contemplated in section 27(3); or
> *(b)* requested by a police official in terms of section 30(3) or 31(4), 12 to, subject to the direction and control of the police official, assist a police official with the search for, access or seizure of an article.[268]

In the writer's view the police official is now tasked with solely conducting the search and seizure of electronic evidence without the option of requesting assistance from a

[265] As discussed in Chapter 2.
[266] Section 26 and Section 27(1) of the Bill.
[267] Section 27(3) of the Bill.
[268] Section 1 of the Bill.

cyber inspector. The Bill's consequent omission of the role of cyber inspector and providing for the generality of an investigator avoids limiting the scope of its application to only a certain role as the ECT Act did. Therefore, it is submitted that this a positive step in changing the current position. The reason is that currently police officials are carrying out search and seizure of electronic evidence in the investigation of crime therefore the Bill now enhances their existing powers to perform cyber specific procedures independently. The implication, however, is that police officials require specialised training to apply the provisions of the Act.

Further structures that the Bill provides for with regard to assistance in investigation of cybercrime is the 24/7 Point of Contact and the Cyber Response Committee. The creation of the 24/7 Point of Contact as envisaged by the Bill is inspired by the Cybercrime Convention[269] setting out its features to include operating twenty-four hours a day and seven days a week.[270] The objective of this organisation is to ensure that assistance is available with regard to proceedings or investigations of any offence as set out in the Bill.[271]

The type of assistance that can be expected from the 24/7 Point of Contact consists of technical advice, legal assistance, identification and location of an article and/or suspect and cooperation with authorities in foreign jurisdictions.[272] In addition, all requests for assistance and cooperation from foreign states must go through the 24/7 Point of Contact who will then submit said request to the NDPP[273] for consideration.[274]

The Cyber Response Committee is established by the Bill with the object of implementing cybersecurity policies created by Government.[275] The centralisation and

[269] MA Vatis 'The Council of Europe Convention on Cybercrime' (2010) *Proceedings of a workshop on deterring cyberattacks* 217.
[270] Section 50 (3) (a) of the Bill.
[271] *Ibid.*
[272] Section 50 (3) (b) of the Bill.
[273] National Director of Public Prosecutions.
[274] Section 46(1) and (2) of the Bill.
[275] Section 53 (1) and (5) of the Bill.

proper coordination of these two bodies will ensure effective investigation and regulate cybercrimes.[276]

Currently, South Africa has a Cybersecurity Hub[277] that took 3 years to establish and an initiative known as the Cybercrime.org.za.[278] It is submitted that the 24/7 Point of Contact and Cyber Response Committee will be established albeit in the far future. In my view, this is as a result of the lack of both human and financial resources to set up and staff these centres.

The opinion of the Director of Centre for Cyber Security situated at the University of Johannesburg is that South Africa does not have the capacity for effective cybersecurity.[279] Inasmuch as the Bill provides good ideas and structures to deal with cybercrime, there is doubt as to whether South Africa actually have the people and/or resources to implement it.[280]

2.4. Specialised Training

The investigation of cybercrime can be a lengthy process and therefore requires a significant allocation of resources.[281] In addition to monetary resources required to track suspects, trained investigators that are skilled and educated in cybercrime are also required.[282] Cybercrime investigators must be equipped not only to collect electronic evidence but also analyse said evidence and be able to communicate it before a court of law.[283] The reality is that specially trained cybercrime investigators are far and few resulting in the lack of investigations and prosecutions.[284]

---

[276] M Musoni (note 232 above, 687).
[277] DP Van der Merwe et al (note 12 above, 66).
[278] Cybercrime.org.za available at *http://cybercrime.org.za/,* accessed on 1 October 2017.
[279] E Goff 'SA doesn't have the people to fight cybercrime, warns expert' 23 May 2017 *IOL* available at http://www.iol.co.za/business-report/companies/sa-doesnt-have-the-people-to-fight-cybercrime-warns-expert-9300956*,* accessed on 1 August 2017.
[280] *Ibid.*
[281] Hill and Marion (note 10 above, 92).
[282] *Ibid.*
[283] *Ibid.*
[284] *Ibid.*

Further to these structures, it is necessary that law enforcement agencies are sufficiently equipped to make use of investigative tools and possess knowledge on the nuances of the law to avoid investigations being hindered and jeopardise the fairness of a trial.[285] One of the investigative tools is computer forensics which entails the examination of various computer components such as external drives, printers, hard drives; and the examination of electronic evidence such as data traffic, and stored data.[286]

The investigation of an alleged cybercrime scene requires specialised knowledge and expertise.[287] South Africa acknowledging the threat of cybercrime requested assistance from the Council of Europe in the form of improving capacity by the implementation of legislation.[288] Thus the judiciary have already received cybercrime specific training equipping them to effectively apply cyber principles to the matters they preside over.[289] It is expected that law enforcement agencies would receive further training that will equip them with necessary cybercrime related information.[290]

The future establishment of the specialised organisations such as the 24/7 Point of Contact and the Cybersecurity Response Committee requires its members to undergo training extensively in the field of cybercrime in order to effectively carry out their functions. According to the Bill, prosecutors who possess the required knowledge and skills to address any aspect relating to the Act must be available to provide legal assistance when necessary or expedient to the 24/7 Point of Contact.[291] It is submitted that as technology advances continuously, ongoing training should be completed by all stakeholders involved in and affected by the cyber related matters. These include law enforcement, legal professionals, judicial officers, court officials and interpreters.

---

[285] V Basdeo (note 205 above, 7).
[286] Hill and Marion (note 10 above, 13).
[287] DP Van der Merwe… et al (note 12 above, 66).
[288] G Makhafola 'Training to help SA tackle cyber crime' 11 April 2016 available at *http://www.iol.co.za/news/crime-courts/training-to-help-sa-tackle-cyber-crime-2007868*, accessed on 22 June 2016.
[289] *Ibid.*
[290] T Mochiko 'Bill takes aim at porn and cyberbullying' 20 January 2017 available at *https://www.businesslive.co.za/bd/national/2017-01-20-bill-takes-aim-at-porn-and-cyberbullying/,* accessed on 12 May 2017.
[291] Section 50 (5) of the Bill.

2.5. Search warrants in terms of Bill

As discussed in the previous chapter,[292] a valid warrant sets out with sufficient particularity the details regarding the search and seizure such as the premises or container to be search, describes the article and the like.[293] However, the Bill states that a police official may search and access "an article identified in the warrant to the extent set out in the warrant."[294] This provision may have constitutional implications in that there is no limitation placed on the search which leaves the individual vulnerable to their personal information being accessed and violated.[295]

It is submitted that this provision of the Bill has both positive and negative implications. On the positive side, in alignment with the nature of electronic evidence being intangible and its identity being difficult to ascertain, police officers have the leeway in describing the article to be seized in the warrant without the validity of the warrant being questioned. This allows police officers to conduct investigations in instances where they are uncertain of what the electronic evidence is and can search all devices instead of being restricted. However, warrants should not be too broad or vague as this may result in the warrant being declared null and void and set aside.[296]

Currently, it is noted that the 'Interim Standard Operating Procedures Dealing with Electronic Evidence' and the 'Practical Guide to Apply for Search Warrants in terms of the Provisions of Section 21 of the Criminal Procedure Act' provide guidance to police officials to describe articles using the descriptions set out in the ECT Act such as "data", "data message" and "information system".[297]

Another point to mention is that the Bill now changes a factor under which a search warrant is issued. Currently, the CPA instructs that a magistrate or justice issue a warrant based on reasonable grounds of belief that the article to be seized is within

[292] As discussed in paragraph 2.2.2 (a) of Chapter 2 of this dissertation.
[293] *Minister of Safety and Security v Van der Merwe* 2011 (2) SACR 301 (CC).
[294] Section 27 (e) and (f) of the Bill.
[295] *Ibid.*
[296] As discussed in paragraph 2.2.2(b) of Chapter 2 of this dissertation.
[297] DC Myburgh (note 274 above, 111).

the area of his/her jurisdiction.[298] This was seen as ineffective in law enforcement as it resulted in the application of multiple warrants in respect of networked environments in cyberspace.[299] The Bill now states that a magistrate or justice may issue a warrant on reasonable grounds of belief that an article is 'within the Republic, if it is unsure within which area of jurisdiction the article is being used or is involved in the commission of an offence.'[300]

In the writer's view, this is a positive change to the current position as cybercrime takes place and electronic evidence lives in the cyber realm. With information on the internet being global, borderless and faceless,[301] deciding the territory in which the crime was committed or where the electronic evidence is located is not an easy undertaking.[302] The Bill caters for mutual assistance in Chapter 6 to further mitigate against the trans-border nature of electronic evidence.[303]

Therefore, the search and seizure of electronic will be hastened without the excessive and uncertain procedure of first determining jurisdiction and then making applications for the necessary warrants. It is submitted that there is no judicial insight relating to this matter as the Bill is yet to be promulgated and warrants of this nature have yet to be applied for.

2.6. Constitutional right to privacy and right to a fair trial

The Bill specifically addresses privacy concerns by stating that the search and seizure powers bestowed upon police officials must be subject to 'strict regard to decency and order; and with due regard to the rights, responsibilities and legitimate interests of other persons in proportion to the severity of the offence.'[304] It is submitted that this provision

[298] Section 21 (1) (a) and Section 25(1) of the CPA.
[299] Basdeo (note 41 above).
[300] Section 27(1) (a) (bb) of the Bill.
[301] S Papadopoulos et al. (note 7 above, 334).
[302] S Brenner and BJ Koops 'Approaches to Cybercrime Jurisdiction' (2004) 4 (1) *Journal of High Technology Law* 11.
[303] This entails requesting or providing information to foreign states. The Bill applies in addition to Chapter 2 of the International Co-operation in Criminal Matters Act, 1996.
[304] Section 34 (1) (a) and (b) of the Bill.

is in line with the Constitution as it provides as a safeguard against the invasion of privacy.

The Bill further imposes an obligation on any person to provide technical or other assistance to a police official in order to conduct search and seizure procedures if required.[305] Currently, under the ECT Act this obligation extends to the accused person whereby should the accused refuse to assist (for example by means of providing a password to unlock the electronic device) he/she would be guilty of an offence.[306] This contradicted the right to a fair trial and the suspect's privilege against self-incrimination.

The difference between the Bill and the current legislative position is that the Bill specifically states that the person who is suspected to have committed the offence and is the subject of that investigation is not required to assist the police in this regard.[307] It is submitted that this new feature in the Bill addresses the previous challenge posed by the ECT Act and complies with the constitutional requirements of the right to a fair trial and the privilege against self-incrimination.

2.7. Surveillance mechanisms used as search and seizure methods

The introduction of Regulation of Interception of Communications and Provision of Communication Related Information Act (RICA)[308] was pivotal in addressing information gathering[309] of crime that was committed on the internet.[310] This Act establishes the practice of surveillance of direct and indirect communications and the collection of information.[311] This is done by interception, monitoring, data retention

[305] Section 32 (1) of the Bill.
[306] Section 82 (2) of the ECT Act.
[307] *Ibid.*
[308] Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002 (hereinafter referred to as "RICA").
[309] This is a method of investigation. S Papadopoulos…et al. (note 7 above, 339).
[310] *Ibid,* 345.
[311] *Ibid.*

and decryption.[312] It further brought about the prohibition of unlawful data interference or monitoring of data.[313]

Currently, the exceptions to the general prohibition of unlawful interception is, amongst others: a directive being granted permitting the interception; consent being provided; for reasons such as the prevention of serious bodily harm or to determine location in emergency situations etc.[314]

RICA provides for different directions and warrants, namely:

- Interception direction;[315]
- Real-time communication-related direction;[316]
- Archived communication-related direction;[317]
- Decryption direction;[318]
- Entry warrant.[319]

RICA is the only law in South Africa that governs communications signal interception.[320] Interception of communication between two persons where consent is not provided is illegal if it is not approved by a judicial officer in terms of RICA.[321] There are two types of interception that operates in South Africa. The first is bulk interception which involves ongoing monitoring of the communications of a large section of the population.[322] The second is targeted inception which involves specific monitoring of a certain individual or group of individuals for a defined period of time.[323]

---

[312] *Ibid.*
[313] S Snail 'Cyber Crime in the context of the ECT Act: hacking, cracking, and other unlawful online activities', 2008(16) *Juta's business law* 64.
[314] Section 3 to Section 11 of RICA.
[315] Section 16 of RICA.
[316] Section 17 of RICA.
[317] Section 19 of RICA.
[318] Section 21 of RICA.
[319] Section 22 of RICA.
[320] H Swart 'Communications Surveillance by the South African Intelligence Services' 2016 available at http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf, accessed on 2 December 2017.
[321] *Ibid.*
[322] *Ibid.*
[323] *Ibid.*

The Bill now builds on and works together with RICA by introducing additional directions.[324] The Bill changes the current legal position by setting out specific obligations on all electronic communications service providers[325] whereas currently only fixed line operators were required to be interceptable and store communication-related information.[326]

Further to the above directions and warrant, the Bill creates three more directions that involve data that is reasonably believed to be involved in the commission of an offence[327], namely:

- expedited preservation of data direction - this direction involves preserving data for a period of 21 days.[328]
- preservation of data direction - this direction serves as a less invasive measure than seizure and serves as an alternative means of investigation in instances where seizure of the article in question is not necessary.[329] Under this direction data must be preserved for the period stipulated in the direction which cannot exceed 90 days. [330]
- disclosure of data direction[331] – this direction is similar to that of the preservation of data direction in that it acts as an alternative to seizure of an article.[332]These preservation directions cater for instances whereby the electronic communications service providers is directed to freeze traffic data associated with an identified internet user for a certain period of time for a specific criminal investigation.[333] Preservation relates to data that has already been stored.

[324] Section 38 of the Bill.
[325] Memorandum on the objects of the Cybercrimes and Cybersecurity Bill (2017) (note 26 above, 25).
[326] S2 of Government Notice No. 1325 of 2005 available at *http://www.justice.gov.za/legislation/regulations/r2005/gg28271_r1325_interception-directives.pdf*, accessed on 5 November 2017.
[327] Memorandum on the objects of the Cybercrimes and Cybersecurity Bill (2017) (note 26 above, 13).
[328] Section 39 of the Bill.
[329] Memorandum on the objects of the Cybercrimes and Cybersecurity Bill (2017) (note 26 above, 14).
[330] Section 40 of the Bill
[331] Section 42 of the Bill
[332] Memorandum on the objects of the Cybercrimes and Cybersecurity Bill (2017) (note 26 above, 16).
[333] S Papadopoulos et al. (note 7 above, 341).

It is submitted that these directions are put in place as measures to ensure the availability or integrity of the evidence by preventing deletion, deterioration or modification.[334] This serves as an enhancement of the current legal position and provides a more effective tool in the search and seizure of electronic evidence.

However, it is submitted that, a criticism of these directions is that it imposes obligations on electronic communications service providers and financial institutions to develop their technology and systems to cater for the functionality to give effect to the direction.

3. Conclusion

It is submitted that the Bill aims to achieve the goal of addressing the lacunas in the current legislation and thereby resulting in successful prosecutions of cybercrime. However, this is dependent on whether the government is able to implement the provisions of the Bill by allocating the necessary resources required.

Ultimately with focus specifically on the search and seizure of electronic evidence, it is submitted that the Bill addresses the gaps in the current legislation by providing mechanisms catered towards electronic evidence. It further provides clarity of the definition of cyber specific terminology that also includes specific procedures associated with electronic evidence, however these definitions have yet to be interpreted and adjudicated upon.

It is also beneficial to mention the new mutual assistance provisions that the Bill provides in its Chapter 6. These provisions refer to the International Co-operation in Criminal Matters Act[335] and sets out requirements and procedures in both instances of South Africa requesting assistance from foreign states as well as foreign states requesting assistance from South Africa.[336] However, mutual assistance does not fall

[334] A Nieman (note 100 above, 56).
[335] 1996.
[336] Memorandum on the objects of the Cybercrimes and Cybersecurity Bill (2017) (note 26 above, 31).

within the scope of this research paper and is a broad enough to form standalone subject matter.

Overall, the promulgation of the Bill in essence does not change the existing legislation but merely provides additional mechanisms that brings South Africa on par with technology even though technology is advancing at a faster rate that the law.

CHAPTER FOUR - INTERNATIONAL BEST PRACTICE REGARDING SEARCH AND SEIZURE OF ELECTRONIC EVIDENCE

1. Introduction

One of the reasons behind the introduction of formal cybercrime laws was the landmark incident of the early cybercrime attack, the 'I LOVE YOU' virus which was released in the year 2000.[337] This virus took the form of an email entitled 'I LOVE YOU' which, when opened, swept through the victims' computers destroying files and furthermore scanned the computers for passwords and log in credentials.[338] The effect of this one virus resulted in damage worth billions of dollars and the interruption of corporate networks globally.[339]

At the time of the occurrence of this incident the Philippine suspect could not be prosecuted in terms of any existing statutory cyber-crime, as this conduct was not criminalised according to law of the Philippines.[340] Through this large scale cyber-attack, it became evident that traditional laws were not equipped to deal with modern day crime on the internet which resulted in the culmination of various legal instruments being drafted.[341]

[337] S Papadopoulos et al. (note 7 above, 338).
[338] SC Sprinkel 'Global Internet Regulation: The Residual Effects of the ILoveYou Computer Virus and the Draft Convention on Cyber-Crime' (2002) 25(3) *Suffolk Transnational Law Review* 493.
[339] *Ibid.*
[340] S Papadopoulos et al. (note 7 above, 338).
[341] S Papadopoulos et al. (note 7 above, 338).

A working group was established by Legal Ministers of various Commonwealth jurisdictions in 2000 to develop a model law that caters for electronic evidence and cyber-crime.[342] The Commonwealth Model Law[343] which took guidance from the legislation of Singapore and Canada was concluded in 2002. It specifically addresses search and seizure by stating that warrants may be issued to law enforcement officers, giving them the authority to search and/or seize computer data.

The African Union Convention defines a framework in respect of standard proceedings that relate to information and telecommunications technologies.[344] Further, this Convention provides conditions that should apply to the institution of proceedings specifically to cybercrime.[345] Each State Party is prompted to adopt legislation that creates substantive ICT criminal offences and procedural measures to investigate and prosecute offenders as well as to afford legal capacity and statutory authority to institutions to perform functions such as forensic investigations and prosecutions relating to cybercrime.[346] Even though South Africa has neither ratified nor signed the African Union Convention,[347] it can take guidance from the provisions in the African Union Convention to inform the development of its own local legislation.

The International Organisation on Computer Evidence proposed Principles for the Procedures Relating to Digital Evidence which serves as a solid foundation on which the handling of digital evidence can be based.[348] These principles include, *inter alia*, elements of maintaining the integrity of the evidence, specialised training, and documentation of the search and seizure process.[349]

In relation to the aspect of search and seizure of electronic evidence, one of the more practical guidance notes was created by INTERPOL, which provides insight into

[342] M Gercke *Understanding cybercrime: phenomena, challenges and legal response* ITU (2012) 27.
[343] Commonwealth Computer and Computer-related Crimes Model Law, 2002.
[344] African Union Convention on Cyber Security and Personal Data Protection, 2014.
[345] *Ibid.*
[346] Article 25 of the African Union Convention on Cyber Security and Personal Data Protection, 2014.
[347] African Union, Convention on Cybersecurity and Personal Data Protection Status List available at https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf.
[348] X Lai et al. *Forensics in Telecommunications, Information and Multimedia* (2011) 227.
[349] G8 Proposed Principles for the Procedures Relating to Digital Evidence, High Tech Crime Sub-Group, G8.

aspects such as the phases of digital forensic investigations, challenges faced in the performance of search and seizure of digital evidence and corresponding potential solutions.[350] Digital evidence being in the binary or analogue format goes further than the traditional computer based information.[351] Therefore, one academic view is that, stretching and applying existing rules that govern conventional investigations of physical environments to digital evidence is inadequate.[352]

It is beneficial for South Africa to have insight that is provided by the above guidance that has already made headway in this field. As the search and seizure of electronic is developing and dynamic area, South Africa should take guidance from abroad and must review international law developments. INTERPOL and the G8 illustrates practical recommendations to the search and seizure of electronic evidence which can feed into the drafting of Standard Operating Procedures for local law enforcement agencies in South Africa.

2. The Cybercrime Convention[353]

In addition to the above, the Convention on Cybercrime published by the Council of Europe is arguably the most relevant international cyber related legal instrument. The Convention was held in Budapest and was passed in June 2001 by the European Committee on Crime Problems.[354] The Cybercrime Convention aims to, amongst other provisions, provide for domestic criminal procedural law powers that are required for investigation and prosecution of cybercrime and the collection of electronic evidence; and making provision for administration of international co-operation.[355]

---

[350] P Reedy "Digital Evidence, 2013-2016" 2016 *18th INTERPOL International Forensic Science Managers Symposium Lyon, France* 593.
[351] C Leacock "Search and Seizure of Digital Evidence in Criminal Proceedings" 2008 (5) *Digital Evidence and Electronic Signature Law Review* 221.
[352] *Ibid.*
[353] Council of Europe Convention on Cybercrime *European Treaty Series – No. 185* (note 76 above).
[354] NE Marion 'The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation' *International Journal of Cyber Criminology* (2010) 4 701. See also MA Vatis (note 276 above, 209).
[355] Explanatory Report to the Convention on Cybercrime *European Treaty Series No. 185* (note 77 above).

South Africa, has not ratified[356] the Cybercrime Convention yet but is a signatory to it meaning that it is not bound by the obligations of the Cybercrime Convention. However, Van der Merwe advises that South Africa has complied, through the ECT Act, with substantive treaty obligations,[357] but has not yet complied with the international obligations (and is not required to) by not passing any legislation giving effect to the procedural law provisions.[358] One of which being Article 19 where search and seizure of tangible objects must be equivalent to the search and seizure procedures of electronic data.[359]

In my view, South Africa has analysed the requirements and recommendations set out in the Cybercrime Convention in the context of South Africa and drafted local legislation that will give effect to those requirements while simultaneously satisfying the South Africa's socio-economic factors and political plight. This will be effected by the promulgation of the Bill which is expected to occur in 2018. It is submitted that once the Bill is enacted then South Africa would in essence be fully compliant with the requirements set out in the Cybercrime Convention.

The Cybercrime Convention attempts to bring traditional concepts and cyber related terminology into alignment.[360] This is depicted in the introduction of new terminology such as 'search or similarly access'.[361] The Cybercrime Convention defines search as 'to seek, read, inspect or review data' whereas 'access' is deemed to be a more neutral term which accurately relates to computer terminology.[362] Likewise, the term 'seize and similarly secure' has been introduced.[363] Seize is deemed to include 'the use or seizure of programmes needed to access the data being seized' and similarly secure

[356] F Cassim 'Addressing the spectre of cyber terrorism: a comparative perspective' (2012)15(2) *PER* 23.
[357] DP Van der Merwe … et al (note 12 above; 105).
[358] *Ibid*.
[359] V Basdeo (note 65 above; 210).
[360] Explanatory Report to the Convention on Cybercrime (note 77 above).
[361] *Ibid.* Concepts such as 'search or similarly access' and 'seize or similarly secure' are new to South African criminal procedure as currently the concept of 'search and seizure' exists without catering for the dimension of accessing and securing electronic evidence.
[362] *Ibid.*
[363] *Ibid.*

is said to denote 'other means by which intangible data is removed, rendered inaccessible or its control is otherwise taken over in the computer environment'.[364]

In comparison to South Africa, it is pertinent to note that the concepts of 'similarly access' and 'similarly secure' were not catered for by the ECT Act nor the CPA. However, the new Cybercrimes and Cybersecurity Bill took guidance from the Cybercrime Convention in modelling its terminology after that of the Cybercrime Convention. The Bill defines 'access', 'article' and 'seize' using the same definitions provided by the Cybercrime Convention.[365]

Article 19 of the Cybercrime Convention deals directly with the search and seizure of stored computer data.[366] It ensures that the same efficiency that is achieved by traditional search and seizure procedures is accomplished by the search and seizure of electronic evidence.[367] It does this by providing for the search and seizure of stored computer data which sets out, inter alia, the search and seizure of a computer system and the computer data stored on it; and a computer data storage medium.[368]

Moreover, Article 19 ensures flexibility in investigations by providing that should an investigator come across relevant information that is stored on a different computer system which is not subject to the search, he/she has the authority to search the other system.[369] Similarly, the ECT Act states that a cyber inspector can perform a search on any equipment where he/she has a reasonable cause to suspect that it has been used in connection with any offence.[370] It is submitted that these provisions should be reviewed as it may result in law enforcement taking advantage of this flexibility by going

---

[364] *Ibid.*
[365] Refer to paragraph 3.2.1 of Chapter 3 of this dissertation.
[366] Section two of the Cybercrime Convention can be further studied to uncover the aspects of procedural law that the Cybercrime Convention provides, however, for ensure a focused dissertation, Article 19 was discussed.
[367] M Gercke (note 349 above, 422).
[368] Article 19(1) of the Cybercrime Convention.
[369] Article 19(2) of the Cybercrime Convention states 'Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.'
[370] Section 82 (1) (f) of the ECT Act.

on fishing expeditions rather than using them as a means to ensure complete investigations.

It is interesting to note that the 2015 version of the Bill included a similar provision which allowed a search to be conducted on the premises to the extent that it is was set out in the warrant, implying that the applicant did not need to know the exact location of the article.[371] This provision is not featured in the 2017 version of the Bill which requires the location to be identified in the warrant.[372]

Article 19 further includes the power to 'seize or similarly secure a computer system', 'make and retain a copy of those computer data', 'maintain the integrity of the relevant stored computer data', and/or 'render inaccessible or remove those computer data in the accessed computer system.'[373] As mentioned above, it is submitted that these concepts have been implemented in the drafting of local legislation to enable a clearer and better understanding of these procedures in the cyber world. Further, it is submitted that the provisions of Article 19 provides perspective into the methods and measures that the search and seizure of electronic evidence should entail and guides local legislatures on what to include in their specific cybercrime investigative procedures. For example, seizure includes making copies of data, removal of a data storage medium and rendering inaccessible data as set out in the definition of seize itself.

In addition the Cybercrime Convention makes provision for international co-operation which aligns with the South African International Co-operation in Criminal Matters Act and Chapter 6 of the Bill which sets out provisions pertaining to mutual assistance.[374]

The Cybercrime Convention has been criticised for providing the surveillance method of data preservation whereas South Africa and other European Union countries provide for the surveillance method of data retention.[375] The difference between the

[371] Section 29 (1) (e) and (f) of the Cybercrimes and Cybersecurity Bill, 2015.
[372] Section 27 (2) (b) of the Bill.
[373] Article 19(3) of the Cybercrime Convention.
[374] This has been mentioned in paragraph 3.3 of Chapter 3 of this dissertation.
[375] S Papadopoulos et al. (note 7 above, 341). See also further discussion in paragraph 3.2.7 of Chapter 3 of this dissertation.

two methods is that data retention encompasses the storage of traffic data that is currently generated for all users over a period of time irrespective of whether the person is suspected of a crime and may be kept in the user's possession.[376] Whereas data preservation refers to storage of traffic data specific to a certain user for the purposes of an investigation for a specific crime. This traffic data can only be preserved for a limited period and must be protected against modification, deletion, or deterioration.[377]

Moving on from the Cybercrime Convention, it is advantageous to narrow down the view to specific jurisdictions to be able to gain a more practical understanding of how search and seizure of electronic evidence is dealt with internationally. For this purpose, the United States of America and Australia will be used in this comparative research. The United States of America is a nation that must be analysed as it is known for its fast and early development of technology which unfortunately also meant that it fell victim to cybercrime much sooner.[378] As a result the legislature was quick to start creating laws to combat cybercrime.[379]

It is submitted that as a result of the Bill incorporating the provisions of the Cybercrime Convention, South Africa will be compliant and should then ratify the Cybercrime Convention to express its intentions of appropriately dealing with cybercrime in a manner that is in line with international standards.

3. United States of America ("USA")

3.1. Introduction

It is alleged that the United States of America has suffered the most at the hands of cybercrime.[380] The USA became aware of its vulnerability as a result of various forms of online attacks which set off alarm bells among security agencies and law

[376] A Nieman (note 100 above, 178).
[377] *Ibid*, 57.
[378] DP Van der Merwe (note 12 above; 93).
[379] *Ibid*.
[380] *Ibid.*

enforcement agencies.[381] It is for this reason that the USA is at the forefront in respect of the criminalisation of cyber-related offenses and the search and seizure of electronic evidence.[382]

Initially, the USA commercialised the internet by leaving the regulatory governance of the internet to those who formed part of the internet community.[383] However, it was soon discovered that this was not effective which led to the passing of two important statutes in the mid-1980s namely, the Counterfeit Access Device and Computer Fraud and Abuse Act ("CFA Act")[384] and the Electronic Communications Privacy Act ("ECP Act").[385] The CFA Act and ECP Act deals with the substantive aspects of cybercrime.

However, the actual focus of this chapter a comparative analysis is the procedural aspects of search and seizure of electronic evidence which is governed by: the Fourth Amendment;[386] Rule 41 of the Federal Rules of Criminal Procedure;[387] and the USA Patriot Act.[388]

3.2. The Fourth Amendment

The Fourth Amendment reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fourth Amendment can be compared to South Africa's constitutional right to privacy that serves as protection against unlawful search and seizures. In respect of privacy of an individual, the Fourth Amendment prohibits unreasonable and unlawful

[381] A Minnaar (note 224 above, i).
[382] SC Sprinkel (note 349 above, 498).
[383] S Papadopoulos et al. (note 7 above, 338).
[384] Counterfeit Access Device and Computer Fraud and Abuse Act ("CFA Act") 18 USC § 1030 (1986).
[385] Electronic Communications Privacy Act ("ECP Act") 18 USC § 2510-2711 (1986).
[386] The Constitution of the United States, Amendment 4.
[387] Federal Rules of Criminal Procedure. Title VIII. Supplementary and Special Proceedings. Rule 41. Search and Seizure.
[388] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act 36 of 2001 (hereinafter referred to as the 'Patriot Act').

searches and promotes a reasonable expectation that all searches will be conducted having due regard to privacy.[389] The District court advised that the mandate of this Amendment is to showcase that the search and seizure is necessary to collect evidence in the investigation of a crime and that the collection of evidence justifies the invasion of an individual's right to privacy.[390]

With reference to cases involving electronic evidence, the courts had to decide whether the individual had a reasonable expectation of privacy with regard to the contents of their electronic mediums.[391] In response to deciding on a reasonable expectation, the content of the electronic mediums was compared to closed containers such as briefcases and it was concluded that the same reasonable expectation of privacy that an individual possesses regarding the contents of a closed container applies to the data that may be held within an electronic storage device.[392] This translates in practice to imply that data contained on a laptop is subject to a reasonable expectation of privacy.

The Fourth Amendment is important in understanding what may be classified as a search. A challenge was posed to the American courts when deciding if the use of a pen register to capture a number dialed on a telephone constituted a search and infringed on the Fourth Amendment.[393] Ultimately it was concluded that the communications were protected by the Fourth Amendment whereas the capturing of telephone numbers was not as the individual using the telephone service was aware that this information is accessible by the service provider therefore there is no reasonable expectation of privacy.[394] This example shows that there are different types of searches even though no traditional physical intrusion took place.

[389] C Leacock (note 358 above, 222).
[390] *United States v. United States District Court*, 407 U.S. 297, 321 (1972).
[391] N Judish… et al *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 3ed, (2002) 3.
[392] *United States v. Ross*, 456 U.S. 798, 822-23 (1982).
[393] *Smith v Maryland*, 1979.
[394] E Casey (note 194 above, 107).

As technology advanced the courts were faced with further decisions on what constituted a search. In *Kyllo v United States*,[395] the court had to decide whether "the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a 'search' within the meaning of the Fourth Amendment". The court held that surveillance without physical intrusion is a search and if conducted without a warrant will be deemed as unreasonable.[396] It is interesting to note the adaptability of the American courts to extend the meaning of search from only physical intrusions to surveillance. It is submitted that it is beneficial for South Africa to consider and explore the American courts' approach of evaluating the circumstances in which the right to privacy applies and if the use of newly developed technology constitutes a search.

Further, the particularity requirement reflects that warrants that do not describe with particularity the things to be seized renders the warrant invalid and results in a violation of the Fourth Amendment.[397] The Court held that even the adequate description of the things to be searched does not save the warrant.[398] It is advised that in order to satisfy the particularity requirement, search warrants that pertain to electronic evidence should identify/describe the physical hardware that is intended to be seized and/or the class of data/information that is intended to be searched.[399]

The purpose behind the particularity requirement is to prevent searches that are too wide by limiting the search to specific areas and things.[400] Computer searches challenges this limitation as the size of a hard drive with the capacity of forty gigabytes (for example) can store information that equates to approximately twenty million pages.[401] Therefore, whereas, in the natural environment a search can be limited to a physical space such as a house or office, in electronic cases, the search of a computer

[395] 2001.
[396] E Casey (note 194 above, 107).
[397] *Groh v. Ramirez* 540 U.S 551 (2004).
[398] *Ibid.*
[399] N Judish et al (note 398 above, 73).
[400] *Maryland v Garrison*, 480 U.S. 79 (1987).
[401] OS Kerr 'Digital Evidence and the new criminal procedure' (2005) 105 *Columbia Law Review* 285.

can result in searching vast amounts of information bypassing the limitation of the particularity requirement.[402]

In comparison to South African law, currently a warrant is required to state with sufficient detail regarding the search and seizure. However, the proposed Bill moves away from this concept and allows for a search to be conducted for an article to the extent that it is identified in the warrant.[403] It is clear that the Bill proposes a deviation from the norm and whether this deviation is a positive one can only be determined in future once it has been enacted, utilised, challenged and adjudicated upon. As it stands, this provision of the Bill may not pass South African and American constitutional muster.

3.3. Rule 41 of the Federal Rules of Criminal Procedure ("Rule 41")

Legal rules that govern search and seizure of evidence are set out in Rule 41 of the Federal Rules of Criminal Procedure.[404] The Federal Rules of Criminal Procedure govern and are applicable to all categories of criminal proceedings that take place in the federal courts.[405] It can be likened to the provisions of the CPA in South Africa. A provision of Rule 41 is to search electronic storage media, seize electronically stored information, where such media or information is concealed through technological means or where protected computers have been damaged without authorisation.[406]

It is drafted to include electronic evidence in stating that a warrant may be issued to utilise 'remote access to search electronic storage media and to seize or copy electronically stored information' in the event that the location of the information or media is concealed via technological means or in an investigation that relates to media in damaged protected computers.[407] Even though the CPA can be applied to matters concerning electronic evidence, it is interesting to note that USA criminal procedure

[402] *Ibid.*
[403] This is explained in paragraph 3.2.5 of Chapter 3 of this dissertation.
[404] GP Bouwer (note 31 above; 163).
[405] GH Dession "The New Federal Rules of Criminal Procedure: I" 1945 *Yale Law Journal* 694.
[406] Rule 41 (b) (6) of the Federal Rules of Criminal Procedure, 2016.
[407] Section (6) (A) and (B) of Rule 41.

explicitly includes cyber related terminology and procedures leaving no room for doubt. Further, the Bill does not refer to remote searches.

In practice, a remote search would entail software being remotely installed on a device and thereby being able to obtain the IP address and/or the identification of information specific to that device.[408] It is a concern that this provision does not address the constitutional aspects that the Fourth Amendment require, such as specific descriptions in the warrant, resulting in this being left to the interpretation of the courts.[409] As mentioned above, remote searches are also an extension of the traditional concept of a search that South Africa should take cognisance of and maybe even include in the drafting of the Standard Operating Procedures that inform the search and seizure of electronic evidence.

In addition to the application for a warrant the USA has adopted a plain view exception which affords investigators the opportunity to obtain evidence related to a different offence once the search has been executed consistently as per the warrant.[410] The court ruled in favour of the state in a case where evidence was seized based on the contraband being in plain view despite it not being described in the warrant.[411] As discussed above, currently South Africa is aligned as the ECT Act has a similar provision even though it has never been implemented.

3.4. Patriot Act

The Patriot Act was passed by Congress in 2001 in response to the September 11 terror attacks.[412] The Patriot Act is said to improve counter-terrorism efforts in several ways, one of which is by updating the law to address new technologies and threats that may be posed by the cyber realm.[413] Further, the Patriot Act enhances the powers

[408] Advisory Committee on Criminal Rules, 2015 Seattle, WA available at http://www.uscourts.gov/sites/default/files/cr2015-09_0.pdf.
[409] Advisory Committee on Criminal Rules, 2016 Missoula, MT available at *http://www.uscourts.gov/sites/default/files/2016-09-criminal-agenda_book_0.pdf.*
[410] C Leacock (note 358 above, 223).
[411] *U.S. v Habershaw* Criminal No. 01-10195-PBS (D. Mass. May. 13, 2002).
[412] C Doyle 'The USA PATRIOT Act: A legal Analysis' 2002 *Congressional Research Service Report for Congress,* i.
[413] U.S Department of Justice, Preserving Life and Liberty 'Highlights of the USA PATRIOT Act' 2001 available at *https://www.justice.gov/archive/ll/highlights.htm*, accessed on 22 October 2017.

of law enforcement agencies enabling them to search telephone records and email communications.[414] The Patriot Act can be used as a benchmark to measure the South African Cybercrimes and Cybersecurity Bill against as it was drafted specifically to address cyberspace and technology as set out below.

Prior to the Patriot Act, warrants could only be obtained from the district where the intended search was to be conducted,[415] however the Patriot Act now provides that warrants in relation to terrorist activities can be obtained from any district irrespective of where the execution of the warrant will take place.[416] This provision caters for the fact that terrorist investigations span different jurisdictions resulting in law enforcement officers being unnecessarily delayed by applying for multiple warrants in each district.[417] Another provision specific to cybercrime is that computer hacking victims are now allowed to approach law enforcement and request assistance in respect of monitoring trespassers on their electronic devices.[418]

This change in the law brings into alignment the crime of physical trespassing to that of electronic trespassing in the form of hacking and provides victims with the same means of remediation.[419] South Africa can adapt and find support in this approach introduced by the Patriot Act to extend the jurisdiction of the application of warrants relating to electronic evidence to a national level. The proposed Bill already contains this provision as discussed in chapter 3. The implication of this is that the magistrates who grant warrants can do so for searches and seizures that are outside their regional jurisdiction, thereby overcoming the challenge of pinpointing the physical locations of crimes that take place in the virtual realm.

Finally, it is noted that USA experiences a similar challenge to South Africa in terms of the lack of successful convictions.[420] It is submitted that even though the USA had cybercrime specific legislation in place, it was still able to adapt and bring about

[414] V Basdeo (note 204 above, 67).
[415] U.S Department of Justice, Preserving Life and Liberty (note 420 above).
[416] Section 220 of the USA PATRIOT Act, 2001.
[417] U.S Department of Justice, Preserving Life and Liberty (note 420 above).
[418] Section 217 of the USA PATRIOT Act, 2001.
[419] U.S Department of Justice, Preserving Life and Liberty (note 420 above).
[420] NY Conteh and PJ Schmick (note 82 above, 33).

improvements to the existing legislation when gaps were exposed by the 11 September 2001 terrorists' attack. In the same light, South Africa should be able to timeously effect necessary changes in legislation in order to address the lacunas that are exposed at present and those that will become exposed even after the promulgation of the Cybercrimes and Cybersecurity Bill. In addition, South Africa can take guidance on practices such as thermal imaging and remote searches and note how those practices interact with legislation.

4. Australia

4.1. Introduction

Technology also posed manifold problems for Australia in respect of search and seizure resulting in new techniques being employed in the investigation of criminal activity.[421] Similarly to the USA, Australia effected change to its legislation by amending the Crimes Act[422] in 1989 to cater for offences relating to computers.[423]

Further to the Crimes Act, the Electronic Evidence Act[424] sets out the definition of data and electronic records and provides for aspects such as authentication, integrity and admissibility of electronic evidence. For purposes of this research paper the Crimes Act and the Telecommunications (Interception and Access) Act[425] are discussed as they are the core pieces of legislation that deals directly with search and seizure.

4.2. Crimes Act

The Crimes Act can be compared to the CPA and ECT Act. The Crimes Act sets out multiple provisions dealing with search and seizure of evidence in criminal investigations.[426] The Act firstly defines data as 'information in any form; and any program (or part of a program)' and defines data storage device as 'a thing containing

[421] A Mason "Reform of the criminal law in Australia" 1989 *Commonwealth Law Bulletin* 1015.
[422] Crimes Act 1914 (Cth) 1015.
[423] JB Hill and NE Marion (note 10 above, 38).
[424] Electronic Evidence Act, 2002 also cited as the Model Law on Electronic Evidence by the Commonwealth Office of Civil and Criminal Justice Reform.
[425] Telecommunications (Interception and Access) Act 1979 (Cth).
[426]G Urbas and KR Choo (note 83 above, 53).

or designed to contain data for use by a computer.'[427] This reflects how the ECT Act currently attempts to define electronic evidence by defining data.

Furthermore, the evidential material to be searched for needs to be identified in a search warrant[428] and such evidential material includes evidence in electronic form.[429] This direction can bring about defence techniques for example should computer discs be seized without first establishing the presence of evidential material on them, the defence may argue inadmissibility of the evidence as seen in the case of *R v PJ.*[430] Even though this provision does not align with the Cybercrime Convention, it holds law enforcement accountable to ensure that the procedure that it follows in respect of applying for warrants and carrying out the search and seizure is done with due diligence. South Africa has taken the same approach.

Part IAA deals with the general powers of search and seizure but also provides for specific regulations when dealing with electronic evidence in s3K and s3L.[431] Executing officers are allowed to take any equipment onto the warrant premises that is necessary for the examination or processing of a thing that is present on the premises in order to assess if such thing is covered by the warrant and may be seized.[432] Another provision is that 'a thing found at the premises may be moved to another place for examination or processing in order to determine whether it may be seized under a warrant….'[433]

This regulation came under scrutiny in *Hart v Commissioner AFP*[434] where the court concluded that this section did not permit the copying of data files to the storage devices that were brought to the premises and then moved to another location for the purpose of analysis. The drafting of this section resulted in significant limitations being imposed on searches that are conducted solely based on s3K because it does not allow for the above scenario where a device is brought onto the premises for the

[427] Section 3 of the Crimes Act 1914 (Cth).
[428] Section 3E (5) (c) Crimes Act 1914 (Cth).
[429] Section 3C of the Crimes Act 1914 (Cth).
[430] [2006] ACTSC 37.
[431] G Urbas and KR Choo (note 83 above, 53).
[432] Section 3K (1) of the Crimes Act 1914 (Cth).
[433] Section 3K (2) of the Crimes Act 1914 (Cth).
[434] [2002] FCAFC 392.

purposes of copying the data onto it and then taken to a different location for analysis.[435]

A further provision refers to any electronic equipment already present at the warrant premises may be used to access data should that data be deemed on reasonable grounds as evidential material and if that data is then suspected to be evidence then the executing officer may copy the data in question to a device that was brought to the premises and then taken away for analysis.[436] This provision clearly compensates for s3K which led to the decision that the legislation does not intend for the searches to be based on either section and be mutually exclusive but can rely on both sections.[437]

The executing officer may also apply for an order which requires a specific person (whether it be, inter alia, the suspect in the investigation or the owner of the electronic equipment) to assist in accessing, copying or converting the data that is held in a computer or data storage device.[438] These provisions together with other cyber specific provisions were introduced into the Crimes Act by the Cybercrime Act.[439] The above are relevant to South Africa as they can be used as examples of how these provisions work together to address gaps in the law. In a similar manner the provisions of the CPA, the ECT Act and the Bill can be used to holistically cover the search and seizure of electronic evidence. In addition, it is noted that the Bill aligns with Australia to the extent of providing for the copying of data instead of the removal of equipment. However, the Bill contrasts with Australian law by excluding a suspect from the obligation of assisting the police in an investigation thus complying with the South African constitutional right to fair trial.

[435] G Urbas and KR Choo (note 83 above, 55-56).
[436] Section 3L of the Crimes Act 1914 (Cth).
[437] *Egglishaw v Australian Crime Commission* [2006] FCA 819.
[438] Section 3LA (1) of the Crimes Act 1914 (Cth).
[439] Act No. 161 of 2002 as amended 'Australian Government Federal Register of Legislation available at *https://www.legislation.gov.au/Details/C2004C01213.* See also G Urbas and KR Choo (note 83 above, 54).

4.3. Telecommunications (Interception and Access) Act[440]

The TIAA operates in the same manner as RICA in South Africa therefore it is relevant to review this piece of legislation to evaluate if South African legislation is on par with Australian legislation insofar as the interception and monitoring of information is concerned.

An aspect of search now includes surveillance methods as previously mentioned above therefore the TIAA was introduced to govern intercepting telecommunications for the purposes of law enforcement.[441] The TIAA provides for the issuance of two different types of warrants: firstly the telecommunication service warrant which only applies to the interception of a single service at a time such as one telephone number.[442] Secondly, a named person warrant which applies to the interception of multiple telecommunication services that is relevant to a specific person.[443] These interception warrants can be issued in respect of only serious offences which includes cybercrime offences.[444] RICA and the proposed Bill cater for different types of warrants that speak to decryption, entry and preservation of data. In this regard it can be said that South African legislation more extensively provides for surveillance and interception of technology methods.

The relationship between law enforcement and ISPs in Australia is subject to preserving evidence, monitoring internet traffic and providing help in respect of three instances: 1) the enforcement of criminal laws; 2) the protection of public revenue; and 3) the safeguarding of national security.[445] Should law enforcement compel ISPs to assist then a warrant is required.[446] However, the challenge exists in that not all ISPs

[440] Act 1979 (hereinafter referred to as 'TIAA').
[441] S Bronitt "Electronic Surveillance, Human Rights and Criminal Justice" (1997) 3(2) *Australian Journal of Human Rights* 187.
[442] Section 46 of the TIAA.
[443] Section 46A of the TIAA.
[444] Section 5D of the TIAA.
[445] Section 313 of the TIAA.
[446] A Maurushat "Australia's accession to the *Cybercrime Convention*: Is the *Convention* still relevant in combating cybercrime in the era of botnets and obfuscation crime tools?" (2010)33(2) *UNSW Law Journal* 449.

are obliged to record data logs that are used in an investigation to track data transfers.[447]

In South Africa the same relationship exists between law enforcement and electronic communications service providers and financial institutions. To avoid the challenge that Australia experiences, the proposed Bill in South Africa places an obligation on electronic communications service providers and financial institutions to put in place technology that enables the implementation of surveillance and interception. Law enforcement need to be vigilant when conducting a search and seizure as should evidence be gathered in breach of the TIAA, then that specific evidence will be rendered inadmissible.[448]

5. Conclusion

It is clear that international best practice is moving forward at a faster rate that South African legislative practices in terms of the search and seizure of electronic evidence. South Africa is nonetheless developing its future legislation (the Bill as discussed in the previous chapter) taking most of its direction from the Cybercrime Convention.

Due to the drastic increase in cybercrime, it is essential that law enforcement officers and prosecutors understand the procedure of obtaining electronic evidence that is stored in computers.[449] Therefore, the role of law enforcement officers need to include the prevention of and responding to cyber threats and attacks.[450] This can be done by the limitation of the scope of cybercriminals by creating awareness and equipping potentials victims so that they can protect themselves against cybercrime as well as the investigation and the identification of cybercriminals.[451]

With regard to the law of the USA, South Africa should take cognisance of the way in which the American courts address the aspect of reasonable expectation of privacy

---

[447] Parliamentary Joint Committee on the Australian Crime Commission 2004 *Cybercrime.* Canberra Parliament of the Commonwealth of Australia.
[448] Australian Government, Australian Institute of Criminology 'Evidence' 2005 *High Tech Crime Brief.*
[449] N Judish et al (note 398 above, ix).
[450] M Watney 'The evolution of legal regulation of the internet to address terrorism and other crimes' (2007) 3 *TSAR* 509.
[451] *Ibid.*

applicable to electronic storage devices and mediums as well as what constitutes a search in terms of using electronic tools in an investigation and whether or not it is covered by law.[452] Further, it is noted that the promulgation of the Bill will bring South African legislation into alignment with American law by catering for searches that can be executed in a jurisdiction different from where it was granted.

Australia aims to prioritise the adoption of strategies which encourage people to report cybercrime incidents, conducting awareness campaigns, creating reporting portals via the web and introducing cybercrime hotlines.[453] Further, it is submitted that South Africa should pay attention to the surveillance method of investigation used by Australia and the different warrants that can be applied for. It is noted that South Africa will be in contrast to Australian law with the promulgation of the Bill by not subjecting a suspect to the provision of obliging with the request of assistance by the police in an investigation.

CHAPTER FIVE - CONCLUSION

1. Introduction

This dissertation critically analysed the current and future legal position in South Africa regarding the search and seizure of electronic evidence, and is based on the following premise: the lack of cybercrime convictions in South Africa is directly linked to the inadequacy of the current legislation that governs search and seizure of electronic evidence. The following conclusions have been drawn in light of the above.

[452] N Judish et al (note 398 above, 211).
[453] Australian Communications and Media Authority 'An overview of international cyber-security awareness raising and educational initiatives' (2011) available at *http://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_reportoverview_intnl_cybersecurity_awareness.pdf,* accessed on 27 October 2017.

2. Does the current legislation in South Africa adequately address the search and seizure of electronic evidence?

In South Africa, there is no standard definition of electronic evidence. The ECT Act makes provision for “data” and “data message” but does not expressly define what constitutes electronic evidence.

In terms of constitutionality, search and seizure affects the rights to a fair trial and privacy. However, should a search and seizure be carried out lawfully, then the infringement of Constitutional rights is justifiable.

Bouwer submits that search and seizure of electronic evidence is divided into two steps. The first being the search for the physical electronic equipment, and the second being, the removal of the physical electronic equipment to a different location to then undergo a different search and seizure of the electronic evidence that is located therein. As a result of the CPA being designed to operate in the physical world, the search and seizure provisions adequately cover the first step of search and seizure of the physical electronic equipment but fails at the second search where the particularity required is not set out in the warrant detailing, *inter alia*, the identity of the searcher.[454]

In addition, sufficient particularity plays a vital role in the application for a warrant, therefore the articles and premises to be seized must be described with sufficient detail in order for all parties to be aware of the subject of the searches. Currently, it is unclear as to the terminology that is required when describing the articles and premises in the warrant. Consequently, the CPA lacks clarity regarding search and seizure of electronic evidence and requires amendment.

With regard to the ECT Act, it is submitted that even though it provided a degree of clarity and certainty by defining cyber related terminology and search and seizure procedures specific to electronic evidence, it limited the use of this Act to the cyber inspector who never materialised.[455] It is submitted that even if the ECT Act adequately addressed the search and seizure of electronic evidence, the impact of its investigative

[454] GP Bouwer (note 31 above, 166).
[455] *S v Miller* [2015] 4 All SA 503 (WCC) at para 56. See also Papadopoulos et al. (note 7 above, 341).

provisions was never fully realised as a result of it not being practically implemented. However, in spite of the above, SAPS have been carrying out search and seizures of electronic evidence therefore the law is not wholly redundant.[456]

In conclusion, the current legal position regarding the CPA can be applied to the search and seizure of electronic evidence, while the cyber specific investigative provisions of the ECT Act lie dormant and therefore ineffective. It is thus fair to conclude that the current legislative position is not wholly inadequate but is in fact more incomplete. As a result, the current legislation should be amended to provide certainty and consistency in the search and seizure of electronic evidence. However, it is submitted that it does not have to be as the promulgation of the Bill will remedy this.
In addition, with regard the Bouwer's two-step process, it is submitted that a single warrant be used with both searches and seizures clearly identified and all details relating to the different locations and searchers identified with sufficient particularity.

3. Will the proposed Bill change the current legal position in South Africa?

In terms of providing clarity and certainty, the Bill defines cyber terminology that enhances the existing position set out in the ECT Act and the CPA. These definitions leads to a clearer understanding of what constitutes electronic evidence and the processes involved in the seizure of electronic evidence.[457]

One of the main features that will change the existing legal position is that the Bill formally requires the creation and implementation of Standard Operating Procedures that will guide law enforcement regarding the search and seizure of electronic evidence.[458] It is noted that interim standard operating procedures have already been drafted[459] which will inform and accelerate the drafting of the final Standard Operating Procedures.

[456] South African Law Reform Commission, Issue Paper 27, Project 126 (note 95 above).

[457] Section 1 of the Bill.
[458] Section 24 of the Bill.
[459] DC Myburgh (note 274 above, 61).

Another change introduced by the Bill, is the absence of the cyber inspector and reference to police officials. Currently, the ECT Act set out powers that were specifically given to the cyber inspector. In the writer's view, this is a positive change as after the promulgation of the Bill, police officials will have cyber specific powers, such as using decryption keys, computer programs and computer data storage mediums to access and seize an article that is identified in the warrant.[460] This is an important advancement as it extends the powers of the already existing police officials rather than trying to create a new persona that governs the search and seizure of electronic evidence. In addition, the Bill makes provision for the establishment of two new organisations[461] that will assist the police in their investigations.[462]

With regards to a search warrant, a point of growth in the legislation is that now judicial officers can grant warrants to be executed outside their regional jurisdiction to the extent that the warrant is executed within the Republic.[463] This mitigates against the trans-border nature of electronic evidence and the inability to speedily pinpoint its exact location.

The Bill aligns with the constitutional right to a fair trial by not putting a suspect in the position where s/he is obliged to assist the police official with the investigation and provide log in credentials to access the desired electronic evidence. This guards against an accused's right against self-incrimination. Further, the Bill adds to the existing surveillance directions provided for by RICA. Consequently, the Bill amplifies the existing legislation.

The only issue that the Bill may face is that it does not align with the requirement of a warrant describing articles with sufficient detail and particularity. The Bill allows for the search of an article to the extent that it is identified in the warrant.[464] It is submitted that this can result in one of two things: firstly it can prove to be successful in allowing for the search and seizure of articles that the police are unable to accurately describe in

[460] Section 27 (2) of the Bill.
[461] 24/7 Point of Contact and the Cyber Response Committee.
[462] Section 50 and Section 53 of the Bill.
[463] Section 27(1) (a) (bb) of the Bill.
[464] Section 27 (e) and (f) of the Bill

the warrant; or police officials can take advantage of the leniency in descriptions and attempt to do blanket searches covering all their bases instead of being specific in their searches.

Overall, it is concluded that the Bill enhances and amplifies the already existing processes and procedures. It brings about a certain degree of legal certainty in understanding technology and empowers police officials to perform the search and seizure of electronic evidence. The Bill proves that South Africa is adapting and developing its legislation to keep abreast of technology advances. In light of the practical implementation, the Bill is not a quick fix and will not be able to remedy the low investigation and prosecution rate of cybercriminals in the near future. Much has to be done on the part of the government, law enforcement and the judiciary as joint efforts to tackle the implementation head on.[465]

4. Does South Africa align with international best practice and what lessons can be learnt?

The following points can be concluded from the comparison of South African law to international best practice:[466]

- When the Bill is promulgated, South Africa will satisfy the procedural obligations set out in the Cybercrime Convention and should therefore ratify this treaty to display that its attitude towards addressing cybercrime is of a serious nature.

- South Africa currently aligns with the particularity requirement and the specificity that ensures the validity of a warrant. However, the Bill slightly deviates from this in allowing a search for articles that are identified to the extent set out in the warrant. Therefore, it allows flexibility in the knowledge of what is to be searched. This still needs to be adjudicated upon to test its effectiveness in practice.

[465] See paragraph 6.2 below.
[466] All conclusions derived from Chapter 4 of this dissertation.

- South Africa can explore the different types of electronic searches such as remote searches and thermal imaging. This should be included in operating procedures or guidelines for search and seizure of electronic evidence as currently this is lacking. To entrench these types of searches, the existing legislation needs to be amended to cater for same or it should be included in the Bill before it is promulgated.

- Currently in South Africa, legislation permits searches to be executed in the jurisdiction that they were applied for. However, the Bill, which aligns with American law, now caters for the granting of warrants to be executed in a different jurisdiction overcoming the borderless nature of electronic evidence.

- Further, it is noted that prominent issues such as cyber-attacks are addressed timeously by legislative intervention in other jurisdictions which are able to make quick decisions in terms of enacting legislation. South Africa is far from this as the first draft of the Bill was published in 2015 and has yet to be enacted in law.

It is clear that international best practice is moving forward at a faster rate than South African legislative practices in terms of the search and seizure of electronic evidence. South Africa is nonetheless developing its future legislation (the Bill as discussed in the previous chapter) taking most of its direction from the Cybercrime Convention. However, the investigative measures and certain legislative aspects such as what constitutes a search still needs to be addressed.

5. Overall conclusion

In light of the above, there is no need for South Africa to amend the current legislation governing search and seizure of electronic evidence in light of the CPA currently being used to search and seize electronic evidence and the proposed, imminent promulgation of the Bill.

It is submitted that the lack of cybercrime convictions may be attributed to the inadequate implementation of the existing legislation such as the defunct cyber

inspector. Therefore, it is more the practical application of the law than the actual law itself that needs to be improved. Consequently, it is submitted that South Africa needs to attend to the equipping and upskilling of its law enforcement officers with respect to specific computer forensics models and methods of search and seizure of electronic evidence to be able to implement the provisions of the Bill.

6. Recommendations

6.1. Legislative recommendations

It is highly recommended that the promulgation of the Bill be prioritised as it will bring about practical changes in the implementation of search and seizure of electronic evidence. Even though the Bill does not change the current legislation it certainly adds to the existing provisions.

The concept of electronic evidence should be defined and standardised amongst all areas of law to provide clarity and consistency on how the law interacts with this type of evidence. Practical recommendations that speak to investigative tools and measures are set out below:-

In addition, there needs to be significant training and upskilling of law enforcement and other stakeholders. Continuous training needs to occur as cybercrime and electronic evidence is a developing field that is constantly changing therefore stakeholders need to keep abreast with technological developments that may have an impact on this field.[467]

6.2. Practical recommendations

One of the specialist investigative tools used in cybercrime investigations is computer forensics which comprises of four elements, namely, 'identification, preservation, analysis and presentation.'[468] In terms of the procedure of collecting evidence in the context of a cybercrime, it is advised that investigators use the method of firstly seizing

[467] M Gercke (note 354 above, 187).
[468] A R Stanfield *The Authentication of Electronic Evidence* (unpublished LLM Thesis, Queensland University of Technology (2016) 124.

evidence that is stored on third-party servers, next prospective surveillance, and finally forensic investigation of the electronic equipment.[469]

It has been determined that electronic evidence has the following qualities: it is latent in nature similar to biometric and DNA evidence; it can easily and with speed transcend borders; it is fragile in the sense that it can be damaged, destroyed or altered; and it can be time-sensitive.[470] Therefore, the following are examples of some of the precautions that should be taken when seizing electronic evidence: refrain from handling contacts, bending connections and exposing electronic evidence to magnetic fields or extreme heat or cold; and avoid attempting to view the contents of the electronic medium without first obtaining assistance from a qualified computer/forensic analyst.[471]

In the case of *Ohio v Cook*, it was argued that integrity of the data seized was compromised in that the hard drive was placed in a static bag.[472] The court held that in these circumstances the data was intact as it was authenticated that the copy made matched the original.[473] In this case the argument failed, however, it is possible that electronic evidence can be damaged if not carefully seized and stored.[474]

The U.S Department of Justice introduced a forensics process model that sets out four different phases during an investigation.[475] These four phases are collection (search, recognition, collection and documentation); examination (uncovering hidden information); analysis (examination of probative value and significance); and reporting.[476]

---

[469] O S Kerr (note 408 above, 285).
[470] U.S Department of Justice 'Electronic Crime Scene Investigation: A Guide for First Responders' 2001 *NIJ Guide* 6.
[471] National Forensic Science Technology Center "Crime Scene Investigation, A Guide for Law Enforcement' September 2013 available at *https://www.nist.gov/sites/default/files/documents/forensics/Crime-Scene-Investigation.pdf*, accessed on 22 October 2017.
[472] *Ohio v. Brian Cook*, 149 Ohio App. 3d 422; 2002.
[473] *Ibid.*
[474] M Meyers and M Rogers "Computer Forensics: The Need for Standardization and Certification" 2004(3)2 *International Journal of Digital Evidence* 1-11.
[475] V Baryamureeba and F Tushabe (note 36 above, 2).
[476] *Ibid.*

Another proposed model more specific to a digital crime scene consists of four different phases.[477] The first phase is preservation for later synchronisation and further analysis.[478] The second is a survey phase which identifies and separates potentially useful data.[479] The third phase is search and collection which entails use of software tools.[480] The last phase is documentation.[481]

Routine procedures have been developed by digital evidence specialists such as an exact duplication of all information stored on a hard drive to ensure accuracy and string searches.[482] A fundamental of the forensic computing process is the copying of evidence.[483] Therefore search and seizure that applies to a computer system and/or stored device, includes making a copy of the data and maintaining its integrity.[484] Further, string searches are used to mitigate against the difficult task of searching through storage mediums that may contain a numerous amount of data files and information.[485]

[477] *Ibid, 4.*
[478] *Ibid.*
[479] *Ibid.*
[480] *Ibid.*
[481] *Ibid.*
[482] C Leacock (note 363 above, 222).
[483] G Urbas and KR Choo (note 83 above, 50).
[484] A Maurushat (note 458 above, 451).
[485] G Urbas and KR Choo (note 83 above, 53).

Bibliography

1. Primary Sources

1.1. Statutes

Civil Proceedings Evidence Act 25 of 1965

Criminal Law (Forensic Procedures) Act 37 of

2013. Criminal Procedure Act 51 of 1977

Cybercrimes and Cybersecurity Bill 2017

Electronic Communications and Transactions Act 25 of 2002

Forensic DNA Regulations, 2015. Government Gazette No. R. 207. 13 March 2015

International Co-operation in Criminal Matters Act, 1996.

Law of Evidence Amendment Act 45 of 1988

National Cybersecurity Policy Framework for South Africa, Government Gazette No.39475 (2015)

Regulation of Interception of Communications and Provision of Communication Related Information Act (RICA) Act 70 of 2002

The Constitution of the Republic of South Africa, 1996

1.2. Cases

Beheermaatschappij Helling I NV v Magistrate, Cape Town 2007 (1) SACR 99 (C)

Cadac (Pty) Ltd v Weber-Stephen Products Co 2011 (3) SA 570 (SCA)

Fedics Group (Pty) Ltd v Matus 1998 (2) SA 617 (C)

Harvey v Niland 2016 (2) SA 436 (ECG)

Key v. Attorney-General, Cape Provincial Division 1996 (6) BCLR 788 (CC)

Minister of Safety and Security v Van der Merwe and Others 2011 (2) SACR 301 (CC)

Motata v Nair No and Another 2009 (1) SACR 263 (T)

Polonyfis v The Minister of Police (64/2010) [2011] ZASCA 26

Powell No v Van der Merwe No 2005 (1) SACR 317 (SCA).

R v Trupedo 1920 AD 58 at 62

S v Brown 2016 (1) SACR 206 (WCC)

S v Harper 1981 (1) SA 88 (D)

S v Miller [2015] 4 All SA 503 (WCC)

S v Miller & others 2016 (1) SACR 251 (WCC)

S v Ningisa and Others 2013 (2) NR 504 (SC)

Seccombe v. Attorney-General 2002 (2) All SA 185

Thint (Pty) Ltd v National Director of Public Prosecutions and Others; Zuma v National Director of Public Prosecutions and Others 2008 (2) SACR 421 (CC)

Van der Merwe v Additional Magistrate, Cape Town; 2010 (1) SACR 470 (C)

Zoeco System Managers CC v Minister of Safety and Security No and Others 2013 (2) SACR 545 (GNP)

Zuma v National Director of Public Prosecutions 2008 (2) SACR 421 (CC)

2. Secondary Sources

2.1. Books

Bellengere A et al… *The Law of Evidence in South Africa*: Basic Principles Cape Town: Oxford University Press, (2013)

Casey, E *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* 3 ed Elsevier Inc, (2011).

Currie I and De Waal J *The Bill Of Rights Handbook* 6th Ed Juta (2013)

Du Toit E 'Search and seizure of electronic evidence' *Commentary on the Criminal Procedure Act* JUTA *(2016)*

Hiemstra VG *Introduction to The Law of Criminal Procedure* 2ed Butterworths, (1985)

Hill, JB and Marion NE. *Introduction to Cybercrime: Computer crimes, laws, and policing in the 21st century* Santa Barbara, CA: Praeger (2016).

Joubert JJ …et al *Criminal Procedure Handbook* 11ed Juta and Company (Pty) Ltd, (2014)

Judish N… et al *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 3ed, (2002)

Mason, S *Electronic Evidence* 3ed Butterworths (2012)

Mason, S and Seng, D (ed) *Electronic Evidence* 4ed London: University of London School of Advanced Study (2017)

McQuade, S.C *Encyclopaedia of Cybercrime* London: Greenwood Press (2009)

Papadopoulos, S … et al. *Cyberlaw@SA III The law of the internet in South Africa* 3ed Pretoria: Van Schaik Publishers, (2012)

Schwikkard, PJ and Van der Merwe, SE *Principles of Evidence* 4th ed Cape Town: Juta and Company (Pty) Ltd (2016)

Van der Merwe, DP. *Computers and the Law* (2 ed) Cape Town: Juta. 2000

Van der Merwe, CG and JE du Plessis, *Introduction to the Law of South Africa* Kluwer Law International, (2004)

Van der Merwe, DP … et al *Information and Communications Technology Law* 2ed Durban: LexisNexis, (2016)

Zeffert DT et al *The South African Law of Evidence* 5ed LexisNexis, (2003).

2.2. Journal Articles

Baryamureeba, V and Tushabe, F 'The Enhanced Digital Investigation Process Model' 2004 *The Digital Forensic Research Conference* available at *https://dfrws.org/sites/default/files/session-files/paper-the_enhanced_digital_investigation_process_model.pdf* accessed on 6 August 2017.

Basdeo, V 'A constitutional perspective of police powers of search and seizure: The legal dilemma of warrantless searches and seizures' (2009) 3 *South African Journal of Criminal Justice* 403-418

Basdeo V 'A critique of search and seizure in terms of a search warrant in South African criminal procedure' (2015) 30 *South African Public Law* 153-175

Basdeo, VM et al 'Search and seizure of evidence in cyber environments: a law enforcement dilemma in South African criminal procedure' (2014)1 *Journal of Law, Society and Development* 48-67

Basdeo, V 'The Constitutional validity of search and seizure powers in South African criminal procedure' 2009 (12) 4 *Potchefstroomse Elektroniese Regsblad* 310-331.

Basdeo, V 'The legal Challenges of search and seizure of electronic evidence in South African criminal procedure: A comparative analysis' (2012) 2 *South African Journal of Criminal Justice* 195-212.

Bouwer, GP 'Search and seizure of electronic evidence: Division of the traditional one-step process into a new two-step process in a South African context' *South African Journal of Criminal Justice* (2014) 2

Brenner, S and Koops, BJ 'Approaches to Cybercrime Jurisdiction' (2004) 4 (1) Journal of High Technology Law

Bronitt S "Electronic Surveillance, Human Rights and Criminal Justice" (1997) 3(2) *Australian Journal of Human Rights*

Cassim, F 'Addressing the spectre of cyber terrorism: a comparative perspective' (2012)15(2) *Potchefstroomse Elektroniese Regsblad* 381-415

Cassim, F 'Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study' 2009 (12) *Potchefstroomse Elektroniese Regsblad*

Cavelty, MD 'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities' 2014 *Science and Engineering Ethics*.

Conteh, NY and Schmick, PJ 'Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks' *International Journal of advanced Computer Research* (2016) 6(23)

Cowling, M 'Criminal Procedure' 2007 *South African Journal of Criminal Justice*

De Villiers DS 'Old "documents", "videotapes" and new "data messages" – a functional approach to the law of evidence (part 1) (2010) 3 *The Journal of South Africa*

Dession GH "The New Federal Rules of Criminal Procedure: I" 1945 *Yale Law Journal* 694.

Doyle C 'The USA PATRIOT Act: A legal Analysis' 2002 *Congressional Research Service Report for Congress*

Gereda, S L 'The Electronic Communications and Transactions Act' 2006 *Telecommunications Law in South Africa*

Gercke M *Understanding cybercrime: phenomena, challenges and legal response* ITU (2012)

Grobler, M et al 'Preparing SA for Cyber Crime and Cyber Defense' (2013) 11(7) *Journal of Systemics, Cybernetics and Informatics* 32-41.

Hofman, J 'Electronic evidence in criminal cases' (2006) 19 *South African Computer Journal* 257

Hunton**,** P **'**A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement environment**' (**2011) 7 *Digital Investigation*.

Irons, A and Ophoff, J 'Aspects of digital forensics in South Africa' 2016(11) *Interdisciplinary Journal of Information, Knowledge, and Management*

Kerr, O S 'Digital Evidence and the new criminal procedure' (2005) 105 *Columbia Law Review* 285

Kerr, I and Gilbert, D *Information Ethics in the Electronic age: Chapter 20: The role of ISPs in the Investigation of Cybercrime* Tom Mendina and Johannes J Britz (2004)

Kerr OS 'Search warrants in an era of digital evidence: *Symposium: the search and seizure of computers and electronic evidence*' (2005) 75 *Mississippi L J* 85–138.

Lai X et al. Forensics in Telecommunications, Information and Multimedia (2011)

227 Leacock C "Search and Seizure of Digital Evidence in Criminal Proceedings"

2008
(5) Digital Evidence and Electronic Signature Law Review 221

Le Roux-Kemp, A 'Criminal Procedure' (2011) Annual Survey of South African Law

Marion, NE 'The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation' International Journal of Cyber Criminology (2010) 4

Mason A "Reform of the criminal law in Australia" 1989 Commonwealth Law Bulletin 1015

Maurushat A "Australia's accession to the *Cybercrime Convention*: Is the *Convention* still relevant in combating cybercrime in the era of botnets and obfuscation crime tools?" (2010)33(2) *UNSW Law Journal* 449

Meyers M and Rogers M “Computer Forensics: The Need for Standardization and Certification” 2004(3)2 *International Journal of Digital Evidence*

Minnaar, A ‘How organised is cybercrime and can it be called organised crime per se?’ 2015(28) *Acta Criminologica: Southern African Journal of Criminology*

Musoni, M ‘Is cyber search and seizure under the Cybercrimes and Cybersecurity Bill consistent with the Protection of Personal Information Act?’ (2016) 37(3) *Obiter* 684

Omar J, Legal Terminology: Criminal Law, Criminal Procedure and Evidence’ 2016 *South African Law Journal*

Reith, M et al… ‘An Examination of Digital Forensic Models’ 2002 (1) *International Journal of Digital Evidence*\

Schwikkard, PJ ‘Evidence’ 2003 *South African Journal of Criminal Justice*

Shin, Y ‘New Model for Cyber Crime Investigation Procedure’ 2011 (2) *Journal of Next Generation Information Technology*

Sissing, S and Prinsloo J ‘Contextualising the phenomenon of cyber stalking and protection from harassment in South Africa’ (2013)26(2) Acta Criminologica: Southern African Journal of Criminology 15-29

Snail, S ‘Cyber Crime in the context of the ECT Act: hacking, cracking, and other unlawful online activities’, 2008(16) Juta’s business law 63-69

Snail, S., ‘Cyber Crime in South Africa – Hacking, cracking, and other unlawful online activities’, 2009(1) Journal of Information, Law & Technology (JILT).

Sprinkel SC ‘Global Internet Regulation: The Residual Effects of the ILoveYou Computer Virus and the Draft Convention on Cyber-Crime’ (2002) 25(3) Suffolk Transnational Law Review 493

Theophilopoulos, C ‘Electronic documents, encryption, cloud storage and the privilege against self-incrimination’ 2015 *South African Law Journal*

Urbas, G and Choo, KR ‘Resource materials on technology-enabled crime’ 2008 *Australian Institute of Criminology* 28

Vatis, MA ‘The Council of Europe Convention on Cybercrime’ (2010) *Proceedings of a workshop on deterring cyberattacks*

Vincze EA ‘Challenges in digital forensics’ (2016) 17(2) *Police Practice and Research*.

Volonino, P ‘Electronic evidence and computer forensics’ 2003 *Communication of the Association for Information Systems*

Watney, M 'Admissibility of Electronic Evidence in Criminal Proceedings: An outline of the South African Legal Position' 2009 *Journal of Information, Law & Technology.*

Watney M 'The evolution of legal regulation of the internet to address terrorism and other crimes' (2007) 3 *TSAR*

3. Thesis

Basdeo V *A constitutional perspective of police powers of search and seizure in the criminal justice system* (unpublished LLM Thesis, University of South Africa, 2009)

Myburgh DC 'Developing a framework for the search and seizure of digital evidence by forensic investigators in South Africa' (unpublished Magister Commercii in Forensic Accountancy thesis, 2016).

Nieman, A *Search and seizure, production and preservation of electronic evidence*

(unpublished LLD, North-West University, 2006)

Stanfield AR *The Authentication of Electronic Evidence* (unpublished LLM Thesis, Queensland University of Technology, 2016)

4. Online Sources

Australian Communications and Media Authority 'An overview of international cyber-security awareness raising and educational initiatives' (2011) available at *http://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_reportoverview*

_intnl_cybersecurity_awareness.pdf, accessed on 27 October 2017.

Bouwer, G 'ICT policy proposals spell out an attempt to nationalise assets' *Business Day* 2017 available at *https://www.businesslive.co.za/bd/opinion/2017-03-13-ict-policy-proposals- spell-out-an-attempt-to-nationalise-assets/,* accessed on 27 August 2017.

Cybercrime.org.za available at *http://cybercrime.org.za/,* accessed on 1 October 2017.

Department of Justice and Constitutional Development 'Cybercrimes Bill

Released for Comment' Discussion of the Cybercrimes and Cybersecurity Bill (2015) available at *http://www.justice.gov.za/legislation/invitations/CyberCrimesDiscussionDocume nt2015.pdf*

Doyle, K 'Data breaches remain unreported by SA organisation' 15 March 2017 *ITWeb Security* available at *http://www.itweb.co.za/index.php?option=com_content&view=article&id=16022 1:Data-breaches-remain-unreported-by-SA-organisations&catid=234*, accessed on 16 September 2017.

Goff, E 'SA doesn't have the people to fight cybercrime, warns expert' 23 May 2017 *IOL* available at *http://www.iol.co.za/business-report/companies/sa-doesnt-have-the-people-to-fight-cybercrime-warns-expert-9300956,* accessed on 1 August 2017.

Internet World Stats available at *http://www.internetworldstats.com/stats.htm*

accessed on 14 April 2017.

Kruger, Adv J 'Concise Submission on the Draft Cybercrimes and Cybersecurity Bill [B-2015]' 26 November 2015 available *at https://www.ellipsis.co.za/wp-content/uploads/2015/11/151126_cfcr_submission_on_cybercrimes_and_cyber security_bill.pdf*, accessed on 30 September 2017.

Mahlobo, D MP, Minister of State Security 'Remarks on Cybersecurity Symposium' 1 March 2015 available at *http://www.gov.za/speeches/minister-david-mahlobo-cybersecurity-symposium-1-mar-2015-0000,* accessed on 5 April 2017.

Makhafola, G 'Training to help SA tackle cyber crime' 11 April 2016 available at *http://www.iol.co.za/news/crime-courts/training-to-help-sa-tackle-cyber-crime- 2007868*, accessed on 22 June 2016.

Mapisa-Nqakula N 'Justice, Crime Prevention and Security post-SoNA Cluster media briefing' 2015 Government Communications available at *http://www.gcis.gov.za/newsroom/media-releases/justice-crime-prevention-and- security-post-sona-cluster-media-briefing* accessed on 5 August 2017.

Mashiloane, L 'Piet Pieterse: SAPS intensifies cyber crime battle' 2014 available at *http://www.itweb.co.za/index.php?option=com_content&view=article&id=13489 0* accessed on 10 August 2017

Media Briefing: Statement by the Deputy Minister of justice and Constitutional Development, the Hon JH Jeffery, MP on the new proposed Cybercrime and Cybersecurity Bill, 19 January *2017 Department of Justice and Constitutional Development available at http://www.justice.gov.za/m_speeches/2017/20170119-CyberCrimeBillBriefing.html*

Mochiko, T 'Bill takes aim at porn and cyberbullying' 20 January 2017 available at *https://www.businesslive.co.za/bd/national/2017-01-20-bill-takes-aim-at-porn- and-cyberbullying/,* accessed on 12 May 2017.

Mulaudzi T 'SA affected in Global Cyberattack' *Eyewitness News* 13 May 2017 available at *http://ewn.co.za/2017/05/13/sa-affected-in-global- cyberattack,* accessed on 20 May 2017.

Park M 'Meet the FBI's top 5 Most Wanted for cyber crimes' CNN available at *http://edition.cnn.com/2017/03/16/us/fbi-most-wanted-cyber-crimes/index.html,* accessed on 6 August 2017.

Pierce, L 'Cybercrimes Bill – much better in 2017' *IT – Online* available at *https://it-online.co.za/2017/01/25/cybercrimes-bill-much-better-in-2017/,* accessed on 3 June 2017

'South Africa Internet Users' *Internet live Stats* available at *http://www.internetlivestats.com/internet-users/south-africa/,* accessed on 20 May 2017.

'Speech by the Deputy Minister of Justice and Constitutional Development, the Hon JH Jeffery, MP, during the Debate on Vote 21: Justice and Constitutional Development, National Assembly, 19 May 2015' available at *http://www.justice.gov.za/m_speeches/2015/20150519_BudgetVoteDM.html,* accessed on 29 September 2017.

Swart, H 'Communications Surveillance by the South African Intelligence Services' 2016 available at *http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf,* accessed on 2 December 2017.

'TalkTalk hack attack: Friends admit cyber crime charges' BBC News available at *http://www.bbc.com/news/uk-england-stoke-staffordshire-39725208*, accessed on 6 August 2017.

U.S Department of Justice, Preserving Life and Liberty 'Highlights of the USA PATRIOT Act' 2001 available at *https://www.justice.gov/archive/ll/highlights.htm*, accessed on 22 October 2017

'WARNING: Cyber attack may be coming to South African businesses' 28 June 2017 available at *https://www.iol.co.za/business-report/warning-cyber-attack-may-be- coming-to-south-african-businesses-10012176,* accessed on 1 July 2017.

Weideman, R 'Here come the cyber inspectors' (2003) ITWeb Internet *http://www.itweb.co.za/index.php?option=com_content&view=article&id=8131 9* accessed on 21 April 2017

5. Other works of reference

2013 Norton Report, Business Media Mags available at *http://businessmediamags.co.za/sa-ranks-worlds-third-highest-cybercrime- victims-2/,* accessed on 20 July 2017.

Advisory Committee on Criminal Rules, 2015 Seattle, WA available at http://www.uscourts.gov/sites/default/files/cr2015-09_0.pdf.

Advisory Committee on Criminal Rules, 2016 Missoula, MT available at *http://www.uscourts.gov/sites/default/files/2016-09-criminal-agenda_book_0.pdf.*

Australian Government, Australian Institute of Criminology 'Evidence' 2005 *High Tech Crime Brief*

Council of Europe Convention on Cybercrime *European Treaty Series – No. 185* available at *http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf*

Crime Statistics 2015/2016, *South African Police Service Department of Police* available at *https://www.saps.gov.za/services/crimestats.php,* accessed on 5 April 2017.

Cyber Crime and Cyber Security Trends in Africa, 2016 *Global Forum on Cyber Expertise* available at *https://www.thegfce.com/initiatives/c/cybersecurity-and- cybercrime-trends-in-africa, accessed on 14 April 2017.*

Department of Justice and Constitutional Development Notice 871 of 2016, Publication of Explanatory Summary of the Cybercrimes and Cybersecurity Bill, 2017.

Explanatory Report to the Convention on Cybercrime *European Treaty Series No. 185* available at *https://rm.coe.int/CoERMPublicsCommonSearchServices/DisplayDCTMConten t?documentId=09000016800cce5b*

G8 Proposed Principles for the Procedures Relating to Digital Evidence, High Tech Crime Sub-Group, G8.

Memorandum on the objects of the Cybercrimes and Cybersecurity Bill (2017) available at h*ttp://www.justice.gov.za/legislation/bills/CyberCrimesDiscussionDocument201 7.pdf*

National Forensic Science Technology Center "Crime Scene Investigation, A Guide for Law Enforcement' September 2013 available at *https://www.nist.gov/sites/default/files/documents/forensics/Crime-Scene-Investigation.pdf*, accessed on 22 October 2017.

Parliamentary Joint Committee on the Australian Crime Commission 2004 *Cybercrime.* Canberra Parliament of the Commonwealth of Australia

Reedy P "Digital Evidence, 2013-2016" 2016 *18th INTERPOL International Forensic Science Managers Symposium Lyon, France* 593

S2 of Government Notice No. 1325 of 2005 available at *http://www.justice.gov.za/legislation/regulations/r2005/gg28271_r1325_interce p tion-directives.pdf*, accessed on 5 November 2017.

South African Law Commission Discussion Paper 99 (Project 108) 'Computerrelated crime: Preliminary proposals for reform in respect of unauthorised access to computers, unauthorised modification of computer data and software applications and related procedural aspects' (2001).

South African Law Reform Commission, Issue Paper 27, Project 126: Review of the Law of Evidence. Electronic evidence in criminal and civil proceedings: admissibility and related issues (accessed through *http://salawreform.justice.gov.za/ipapers/ip27_pr126_2010.pdf* on 2 July 2017)

The Department of Justice and Constitutional Development *Justice publishes Cybercrimes and Cybersecurity Bill for public comment* 28 August 2015 available at *http://www.justice.gov.za/m_statements/2015/20150828-CyberCrimesBill.html*, accessed on 6 August 2017.

The Department: Public Service and Administration 'Toolkit on Standard Operating Procedures' available at *http://www.dpsa.gov.za/dpsa2g/documents/tenders/DPSA002_2015/TOOLKIT%20ON%20STANDARD*

UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996 available at *https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf*, accessed on 25 August 2017.

U.S Department of Justice 'Electronic Crime Scene Investigation: A Guide for First Responders' 2001 *NIJ Guide*

6. Foreign Law

6.1. Statutes

African Union Convention on Cyber Security and Personal Data Protection, 2014

Commonwealth Computer and Computer-related Crimes Model Law, 2002

Counterfeit Access Device and Computer Fraud and Abuse Act 18 USC § 1030 (1984).

Crimes Act 1914 (Cth)

Cybercrime Act No. 161 of

2002 Electronic Evidence Act,

2002

Electronic Communications Privacy Act 18 USC § 2510-2711 (1986)

Federal Rules of Criminal Procedure, 2016

Telecommunications (Interception and Access) Act 1979 (Cth)

The Constitution of the United States, Amendment 4.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act 36 of 2001

6.2. Cases

Egglishaw v Australian Crime Commission [2006] FCA 819

Groh v. Ramirez 540 U.S 551 (2004).

Hart v Commissioner, AFP [2002] FCAFC 392 (5 December 2002)

Kyllo v United States 2001

Maryland v Garrison, 480 U.S. 79 (1987).

Ohio v. Brian Cook, 149 Ohio App. 3d 422; 2002

R v PJ [2006] ACTSC 37 (2 May 2006)
Smith v Maryland, 1979

U.S. v Habershaw Criminal No. 01-10195-PBS (D. Mass. May. 13, 2002)

United States v. Ross, 456 U.S. 798, 822-23 (1982)

United States v. United States District Court, 407 U.S. 297, 321 (1972)

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

29 June 2017

Mrs Terrina Francine Govender (208504899)
School of Law
Howard College Campus

Dear Mrs Govender,

Protocol reference number: HSS/0933/017M
Project title: A critical analysis of the search and seizure of electronic evidence relating to the investigation of cybercrime in South Africa

Approval Notification – No Risk / Exempt Application

In response to your application received on 27 June 2017, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol has been granted **FULL APPROVAL.**

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment/modification prior to its implementation. In case you have further queries, please quote the above reference number.

PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. Thereafter Recertification must be applied for on an annual basis.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

.....
Dr Shamila Naidoo (Deputy Chair)

/ms

Cc Supervisor: Mr Lee Swales
Cc Academic Leader Research: Dr Shannon Bosch
Cc School Administrator: Mr Pradeep Ramsewak

Humanities & Social Sciences Research Ethics Committee
Dr Shenuka Singh (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 **Facsimile:** +27 (0) 31 260 4609 **Email:** ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za